Eos TR-3235-001

Multilevel Security Systems for Amphibious Operation Command and Control

Phase I Final Report

Contract No: DAAL03-91-C-0003

March 1991

Prepared For:

U.S. Army Laboratory Command
Army Research Office
Research Triangle Park, NC 27709-2211

Prepared By:

B.B. Dillaway
Eos Technologies, Inc.
10116 36th Ave CT SW
Suite 211
Tacoma, WA 98499

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	22 March 1991	Final Report - Nov 90 - Mar 91

4. TITLE AND SUBTITLE
Multilevel Security Systems for Amphibious Operation Command and Control

5. FUNDING NUMBERS
DAAL03-91-C-0003

6. AUTHOR(S)
B. Dillaway

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Eos Technologies, Inc.
10116 36th Ave Ct SW Suite 211
Tacoma, WA 98499-4793

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U. S. Army Research Office
P. O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
ARO 28519.1-EC-SBI

11. SUPPLEMENTARY NOTES
The view, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This study examines multilevel secure (MLS) automation support requirements for the intelligence function of the U.S. Marine Corps tactical command and control system. Design requirements for a system providing multilevel secure operation in accordance with the requirements of DoD 5200.28-STD are developed. This design is consistent with the evolving MTACCS architecture and represents a evolutionary enhancement to the existing Intelligence Automation System (IAS). The design approach makes extensive use of commercially available Trusted software components coupled with developmental Trusted software which implement mission dictated extensions to the commercial product security policy model.

14. SUBJECT TERMS	15. NUMBER OF PAGES
COMPUSEC, INFOSEC, Command and Control, Intelligence, C3I, OPSEC	103
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Foreword

This document represents the results a Phase I SBIR research project by Eos Technologies, Inc. The goal of this project was to analyze the requirements for Multilevel Secure (MLS) automation system support to the intelligence function of the U.S. Marine Corps tactical Command and Control (C2) system and to develop a feasible design approach for implementing such a system. This effort was successful, and the design requirements for a MLS intelligence automation system are identified in this document. These requirements provides a basis for proceeding with a detailed design and prototype system implementation in a Phase II research program.

The results of our analysis are presented in the form of System Segment Specification based on the guidance in MIL-STD-490A. This somewhat unusual format for documenting an initial research effort was requested by the sponsoring agency to better meet their needs.

The contributions of Mr. Gerald Schneider to this project are acknowledged. His expertise in military intelligence operations and familiarity with the MTACCS concept were invaluable and are reflected in the contents of this document.

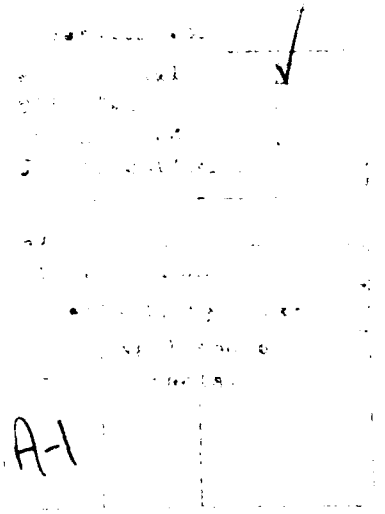

TABLE OF CONTENTS

1.0 SCOPE

1.1 IDENTIFICATION

This document represents a preliminary System Segment Specification (SSS) for a Multilevel Secure Intelligence Automation System (MLS-IAS). This system will form a component of the Marine Air-Ground Intelligence System (MAGIS) and allow the direction, collection, processing and dissemination of multi-source critical tactical intelligence data. It will store and protect information at multiple sensitivity levels and provide for automated simultaneous interface to external systems operating at varying data sensitivity levels. This will provide enhanced flexibility and efficiency in support of the G-2/S-2 staff to conduct their mission (relative to exiting dedicated security mode automation systems) while providing a high degree of protection from compromise and information integrity.

This SSS focuses on the MLS requirements for an IAS and represents an extended set of requirements for the existing AN/TYQ-19(V) Intelligence Automation Systems (IAS). Additional information on operational requirements, design and construction, logistics, personnel and training, subordinate elements, qualification requirements, quality assurance provisions, etc. can be found in the SSS for the IAS Product Improvement Program. These requirements apply to the MLS-IAS unless specifically addressed in this specification. Duplication of material from the SSS for the IAS Product Improvement Program has been minimized. However, extract material has been incorporated where it felt necessary to provide background information and context for the discussion of security requirements.

1.2 SYSTEM OVERVIEW

The purpose of the MLS-IAS is to automate the Marine Air-Ground Task Force (MAGTF) intelligence activities. It will support the automated direction, collection, processing and dissemination of multi-source/multilevel intelligence.

1.3 DOCUMENT OVERVIEW

This specification has been prepared using MIL-STD-490A for guidance and addresses the MLS-IAS security critical elements of the system definition and characteristics. This document is based on the results of a Phase I SBIR program of research. Due to the limited scope of the technical effort feasible under this program, this specification should be viewed as a preliminary and subject to revision and enhancement during subsequent research and development efforts. Section 6 provides a list of acronyms and a glossary of Computer Security (COMPUSEC) terminology.

2.0 APPLICABLE DOCUMENTS

2.1 GOVERNMENT DOCUMENTS

The following documents form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirements.

"Army Tactical Command and Control System (ATCCS) - Common ATCCS Support Software (CASS) System/Segment Specification (SSS)," Army Communications and Electronics Command (CECOM), Fort Monmouth, NJ., 14 December 1990

"MTACCS," Marine Corps Research, Development and Acquisition Command, December 1989 (Draft).

"System/Segment Specification for the Intelligence Analysis System Product Improvement Program (FINAL DRAFT)," Marine Corps Research, Development, and Acquisition Command, Washington, D.C., 25 February 1991.

"Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP)," Volume V Protocol Standard, U.S. Marine Corps, July 1987.

CSC-STD-002-85, "Department of Defense Password Management Guideline," U.S. DoD, 12 April 1985.

CSC-STD-003-85, "Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," U.S. DoD, 25 June 1985.

CSC-STD-004-85, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements --Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," U.S. DoD, 25 June 1985.

DCID 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks (U)," 4 January 1983.

Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," U.S. DoD, 25 June 1985.

DIAM 50-4, "Security of Compartmented Computer Operations (U)," 24 June 1980.

DoD 5200.1-R, "Information Security Program Regulation," August 1982.

DoD 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," revised April 1978.

DoD 5200.28-M, "ADP Security Manual -- Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems," revised January 1979.

DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," U.S. DoD, December 1985.

DoD-STD-2167A, "Military Standard Defense System Software Development," 29 February 88.

DoD-STD-2168, "Military Standard Defense System Software Quality Program," 1 April 87.

FMFM 2-1, "Intelligence"

FMFM 3-20, "Commander's Guide to Intelligence"

FMFRP 3-28, "Tri-MEF Standard Operating Procedures for Field Intelligence Operations"

Marine Tactical Command and Control system (MTACCS) Master Acquisition Plan (MAP) (Draft), 9/11/90.

MCO 1510.58, "Individual Training Standards System for Intelligence Occupational Field"

MIL-STD-490A, "Military Standard Specification Practices,", 4 June 85.

NCSC-TG-001 Version 2, "A Guide To Understanding Audit in Trusted Systems," National Computer Security Center, 1 June 1988.

NCSC-TG-003 Version 1, " A Guide to Understanding Discretionary Access Control in Trusted Systems," National Computer Security Center, 30 September 1987.

NCSC-TG-005, "Trusted Network Interpretation," National Computer Security Center, 31 July 1987.

NCSC-TG-006 Version 1, "A Guide To Understanding Configurations Management in Trusted Systems," National Computer Security Center, 28 March 1988.

NCSC-TG-020-B Version 1."Trusted Unix Working Group (TRUSIX) Formal Security Policy Model for the Unix System (Draft)," National Computer Security Center, July 1990 (Distribution Restricted).

NCSC-TG-021 Version 1(DRAFT), "Trusted Database Management System Interpretation," National Computer Security Center, 22 August 1990.

OH 3-2, "Intelligence"

ROC No. INT 250.1, "Required Operational Capability (ROC) for the Intelligence Analysis System."

2.2 NON-GOVERNMENT DOCUMENTS

IEEE 1003.1, "POSIX Standard System Services," IEEE, 1990.

IEEE P1003.6 Draft 8, "Security Interface for the Portable Operating System Interface for Computer Environments," IEEE, 5 November 1990.

3.0 SYSTEM REQUIREMENTS

The MLS-IAS shall support the United States Marine Corps (USMC) Mission Area 12, Intelligence. Amphibious warfare integrates all types of landing forces, ships, landing craft, aircraft and weapons in a coordinated assault against a hostile shore. The commander of an amphibious task force must have an integrated intelligence picture from all available sources. Some of these sources will be national systems, others will be fleet based systems, and yet other may be systems from co-aligned nations. The net result of the integrated intelligence picture sometimes yields a product that is too highly classified to be releasable to the operational commanders. In such cases, the intelligence function must be able to sanitize these products to provide the information essential to the operational commander at an appropriate classification level. The MLS-IAS must support the flexible and efficient processing of this multi-source, multilevel data in a manner which protects the source data from potential compromise while allowing the generation of operationally useful products.

The MLS-IAS shall be designed to provide MLS operation in accordance with the requirements of DCID 1/16, DIAM 50-4, and DoD 5200.28-STD.

3.1 SYSTEM DEFINITION

The MLS-IAS shall support the formulation of the commander's Essential Elements of Information (EEI's) and Other Intelligence Requirements (OIR), collection management, all-source intelligence analysis and fusion, intelligence production, contingency planning, briefing support, training, and communications connectivity. These missions shall be accomplished by four major functions:

1) Rapid storage and retrieval of all-source intelligence data spanning multiple sensitivity levels (including SCI) data
2) Receipt, dissemination, internal routing, and display of intelligence information
3) Management, tasking, and coordination of organic, theater, and national intelligence collection
4) Provide word processing, spreadsheets, presentation graphics, etc. to facilitate the preparation and dissemination of intelligence products.

The IAS is an integrated intelligence processing system which has many inputs and outputs. The system architecture is evolving as part of the larger MTACCS (Marine Tactical Command and Control System) effort and will have similar hardware and software support. The IAS will have external interfaces to multiple intelligence collection, analysis and production systems. Many of these system are already fielded, some are undergoing evolutionary upgrade, and yet others are planned systems. The system must provide the interface facility to cooperatively provide tasking to these systems and receive their intelligence input.

The MLS-IAS will be designed to provide security control and management of sensitive data. This will include the capability to handle both Special Compartmented Intelligence (SCI) and General Services (GENSER) information. The system will interface to a variety of external elements, via appropriate Marine Corps tactical communications networks, at the Marine Air Ground Task Force (MAGTF) Command Element (CE) level with the Combined Amphibious Task Force (CATF) and other Amphibious Task Force units; with the other components of the MAGIS (TERPES, JSIPS, TCAC); and an intra-MAGTF requirement for communications with other IAS systems at different echelons/units within the MAGTF. A depiction of these interfaces, with the MAGIS elements highlighted, is provided in Figure 3.1-1.

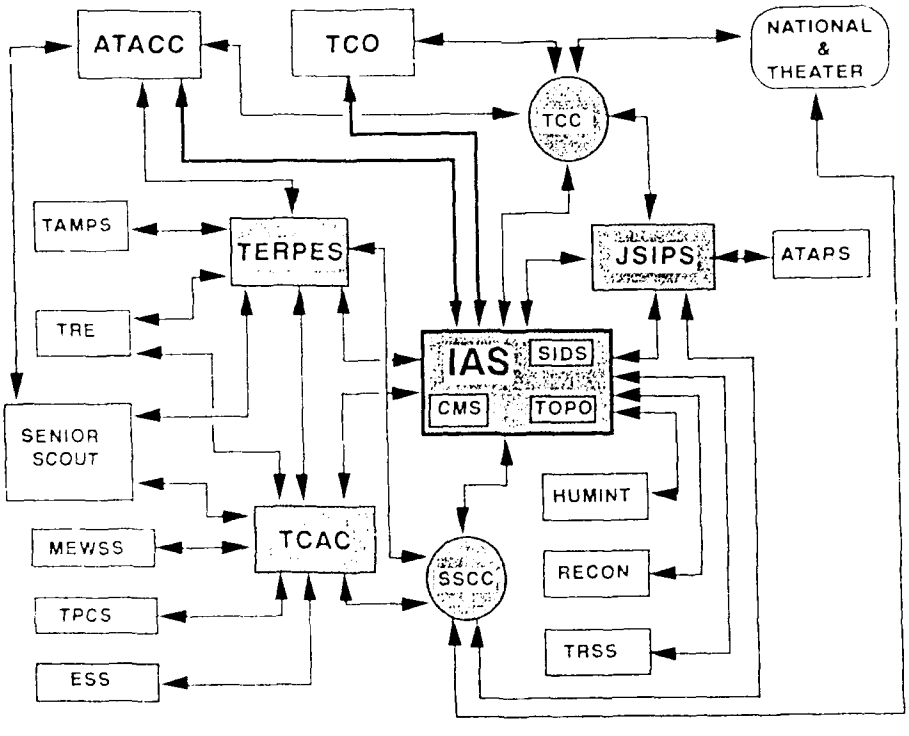

FIGURE 3.1-1. The MAGIS with IAS Interfaces

The MLS-IAS design shall emphasize simplicity and modularity in order to provide a high degree of reliability and maintainability. The system will utilize organic USMC Automated Data Processing (ADP) and/or Non-Developmental Item (NDI) hardware to the maximum extent possible. Commercial Off-the-Shelf (COTS), or previously developed, software shall be used whenever possible. Selected hardware and software will be compatible with the evolving MTACCS standards.

An architecture reference model has been developed by the MCRDAC (Marine Corps Research, Development and Acquisition Command) for development of common MTACCS hardware and software which is designed to support all systems of the MTACCS including the MLS-IAS. This model identifies four layers of common development items as shown in Figure 3.1-2. These layers provide a modular "building block" approach upon which to design MTACCS C4I applications. The lowest layer includes specification of the MTACCS Common Hardware Suite (MCHS). Layer two and three define COTS system support software and command and control support software respectively. These two layers form the MTACCS Common Application Support Software (MCASS). The fourth layer provides the applications environment for both unique MTACCS C4I systems and common applications which may be used across the spectrum of two or more MTACCS C4I systems. This reference model has not yet been fully implemented in the MTACCS programs however it provides guidance for MTACCS developers of future systems. The MLS-IAS design should be consistent with this model.

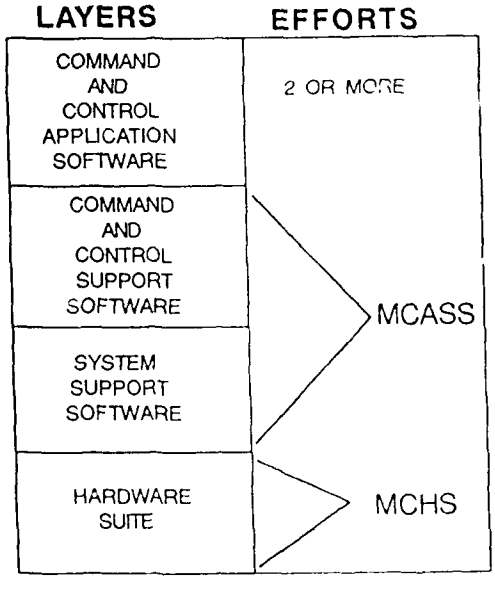

FIGURE 3.1-2. Four Layer MTACCS Hardware and Software Model

Within the four layer model, twelve common application modules are envisioned for the MTACCS. These are shown, along with the other dimensions of an expanded reference, model in Figure 3.1-3. This expanded reference model is still in draft form, but contains recommended near-term hardware and software solutions.

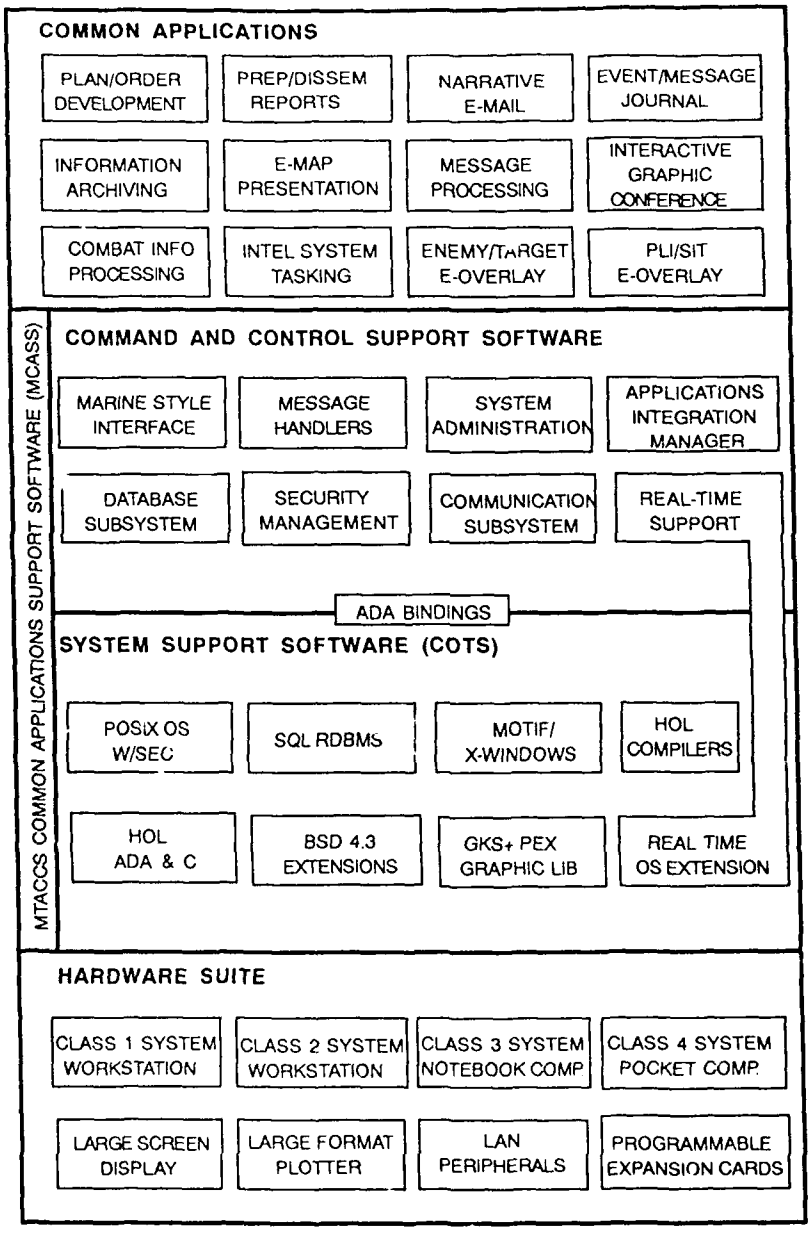

FIGURE 3.1-3. Recommended MTACCS Hardware and Software Architecture

3.1.1 HARDWARE DEFINITION

The MLS-IAS shall be modular and reconfigurable allowing the G-2/S-2 flexibility to configure the system to meet situationally dictated operational requirements. The system will support operations of the G-2/S-2 staff during the conduct of air-ground operations, aboard ship during amphibious operations, and in garrison. Hardware will be compatible with the MTACCS Common Hardware Suite (MCHS) and will minimize the requirement for specialized maintenance procedures. The system will utilize removable secondary storage media (e.g. hard disk drives) to allow sanitization of component elements for storage and transport. The hardware shall provide support for the following functions:

- User input utilizing a keyboard and/or pointing device
- Soft copy output
- Hard copy output
- Bulk data storage of multilevel data
- Bulk data transfer of both multilevel and single level data
- High speed multilevel intra-node data transfer
- Multilevel and single level inter-node data transfer
- Storage, retrieval, and processing of multilevel data
- Complex processing of numeric, textual, and graphical information
- Communications with the USMC tactical communications system
- Communication with USN and national communication systems

The MCHS represents a suite of equipment that spans the total spectrum of Marine Corps tactical requirements. While specific hardware has not yet been selected, these systems are required to be rugged, light-weight and portable. The high end host elements (Class-1) will be a powerful workstation capable of handling the requirements of network server, communications server and high performance data processing facilities. This workstation will be complemented by a workstation (Class-2) of lower, but still significant power and capability. The Class-2 workstation will be usable in conjunction with the Class-1 processor in a LAN environment as well as supporting stand alone deployment. It provides the general purpose capabilities for MAGTF automation.

A third processing element, the Class-3 workstation, is a laptop computer capable of processing, communicating, and serving a network at lower echelons. It will be light weight and Marine portable as a single component. This workstation is complemented by the Class-4 handheld forward entry computer. This computer is a light-weight package appropriate for carrying in the camouflage uniform cargo pocket with sufficient processing capability to displace all current handheld battlefield computers. It enjoys a standard software architecture that is compatible and interoperable with all other computer workstations in this architecture.

These computers are complemented by various peripheral devices to include large screen displays, plotters, CD-Rom storage, printers, and LAN devices. The top three workstations will have a standard bus architecture to allow the insertion of expansion cards in support of intelligent processing support for communications interface requirements. The handheld computer will be tailorable by insertion of "plug-in" memory cards which will support large software libraries.

MEF/MEB MLS-IAS Hardware. The MLS-IAS shall be configurable to support the operational requirements of the MEF/MEB level intelligence staff. The system will be mounted in vehicular shelters and all required power systems and environmental conditioning will be integrated. It shall be possible to enhance the vehicular components through provision of additional user workstations and peripheral devices in a co-located (<50M separation) soft shelter. A minimum of 12 additional workstations will be supported. All vehicular mounted systems will be removable and reconfigurable to allow operation in a building, ship, etc.

The conceptual design of a MEF/MEB MLS-IAS node is shown in Figure 3.1-4 (power and environmental conditioning subsystems are not shown). All processing elements of the system in the node are interconnected via a high speed Local Area Network (LAN). It is desired that the LAN be compatible with the MTACCS LAN (not yet defined). Initial versions of the MLS-IAS will utilize IEEE 802.3 Ethernet LAN technology to take advantage of existing secure network products (see Appendix C).

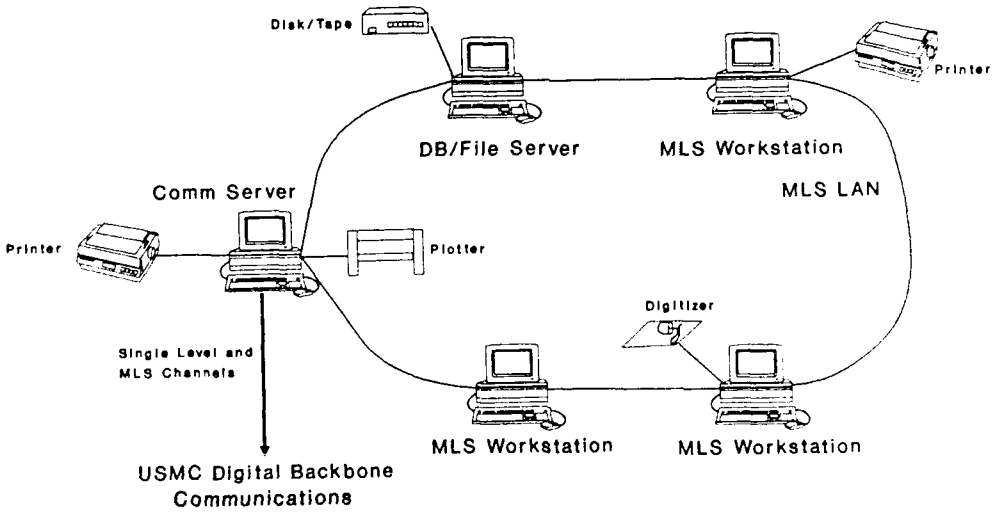

Figure 3.1-4. MEF/MEB Node

There are three distinct processing elements supported in the MEF/MEB node. These provide high performance centralized database and file services, external communications interfaces, and shared peripheral support, and analyst workstations. These processors should be selected to optimized performance for the required functionality and need not be homogenous. Initial versions will utilize processors for which appropriate COTS Trusted components are available (see Appendices A, B, & C).

Supporting peripheral devices include communications interfaces, printers, plotters, digitizer tablets, and magnetic tape/magnetic disk storage devices. It is desired that these elements utilize MCHS hardware when it is defined.

Intermediate MLS-IAS Hardware. The Intermediate MLS-IAS will share common workstations and peripheral devices with the MEF/MEB MLS-IAS. It is intended to be operated in a soft shelter, building, or ship and will be rapidly configurable for these environments. The conceptual design of the Intermediate MLS-IAS is shown in Figure 3.1-5. The system will support a minimum of six analyst workstations.

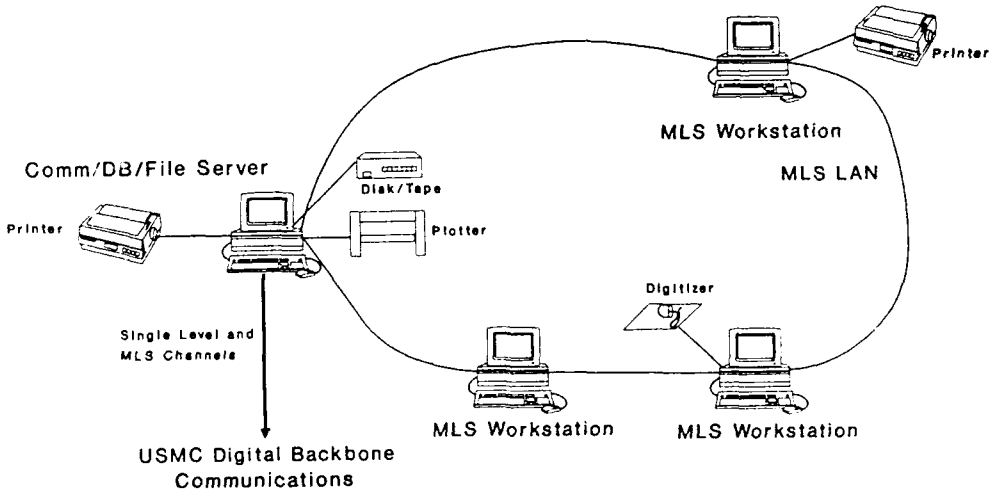

Figure 3.1-5. Intermediate Node

Single Workstation MLS-IAS Hardware. The Single Workstation MLS-IAS shall consist of a single analyst workstation and peripherals as shown in Figure 3.1-6. It will be possible to rapidly integrate a Single Workstation MLS-IAS node in the MEF/MEB or Intermediate node LAN to allow interaction and data exchange with these elements. The Single Workstation MLS-IAS node will be capable of being configured for either MLS or dedicated security mode operation.

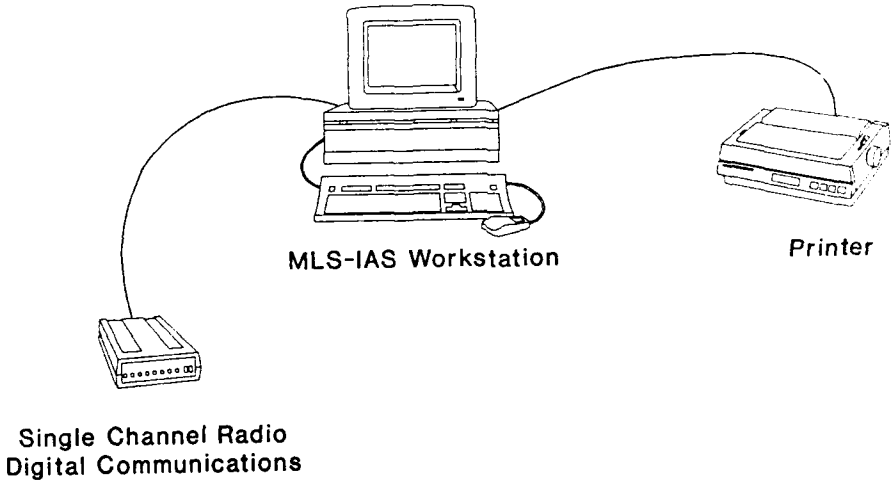

Figure 3.1-6. Single Workstation Node

3.1.2 SOFTWARE DEFINITION

The MLS-IAS software will provide storage, retrieval, transmission, and processing of multilevel data to support the direction, collection, analysis, and dissemination of intelligence information in support of the MAGTF. The system will fully support the concept of multilevel secure computing and will provide:

- Logical separation of data by sensitivity level
- Mandatory and Discretionary Access Controls (MAC and DAC)
- Positive identification and authentication of users
- Auditing of security relevant events
- Support for both single and multilevel external devices

- Separation of duties and least privilege

The MLS-IAS software will be designed around a modular architecture to allow selective capability improvements through module replacement. To facilitate a flexible and adaptable distributed computing environment, extensive use will be made of client-server architectural concepts. The MLS-IAS software will be consistent with the evolving MTACCS Common Application Support Software (MCASS) software standards.

The MCASS component of the reference model is expected to map closely against the emerging results of the U.S. Army CASS architecture development. Because CASS is not yet a mature Army program, it is necessary to make some inference into this development to determine what CASS components might be expected to be useful for the MCASS. Additionally, because of the unique nature of amphibious operations, FMF tailorable contingency structure, and FMF message and communications systems, the MCASS architecture is not expected to map directly to the CASS architecture requirements. Within this document, references to CASS draft security standards are provided to aid in eventual mapping between the MLS-IAS requirements and the MCASS when defined.

The MLS-IAS software shall be structured as shown in Figure 3.1-7, and shall consist of the following elements:

Operating System Software. System software will consist of a Trusted Operating System (OS) and associated peripheral device drivers, MLS file system, MLS resource management, and system maintenance programs. The OS will provide for positive identification and authentication of users on the system, enforce the logical separation of data by sensitivity, and enforce MAC and DAC consistent with DoD security policy.

The OS will be compatible with the POSIX standard interface definition. It is desirable that the OS be compatible with the POSIX security interface standards, however, these are still in preparation. The OS will support clearly defined roles and access rights for a System Administrator (SysAdmin) and applications users in accordance with the principle of least privilege.

Database Management. A Trusted Relational Database Management System (RDBMS) will be provided. The RDBMS will provide for the storage, retrieval, and update of multilevel data. It will serve as the central data repository within the MLS-IAS and will support integrated tools to allow for:

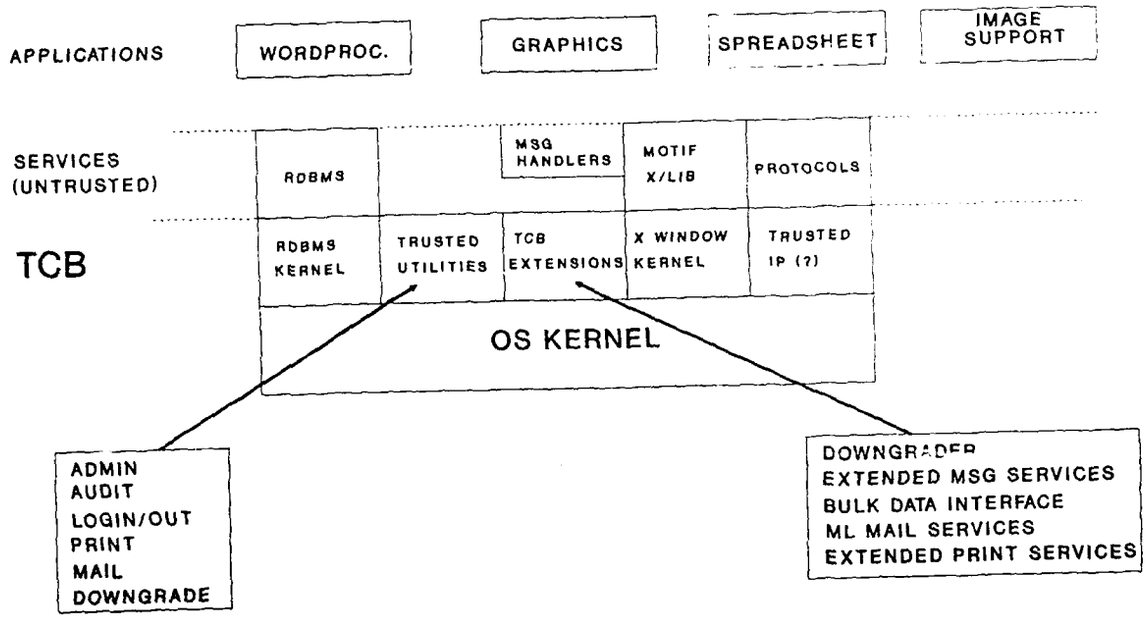

Figure 3.1-7. Software Architecture

- data input validation
- database integrity controls
- event driven stored procedures
- concurrency management
- transaction logging
- error recovery.

The Trusted RDBMS will be configurable to provide the database services on a single workstation, within a distributed multi-workstation environment, and in a distributed environment with a high performance dedicated database server. It is desirable that the RDBMS support data over a range of sensitivities and implement access control mechanisms which are consistent with those enforced by the OS security mechanisms. The RDBMS will support clearly defined roles for the Database Administrator and applications users.

A SQL interface will be provided, extended as required to implement required security functionality. This will be supplemented with 4GL language tools for the

development of data input and retrieval forms and the generation of standardized reports.

Communications. The system will support both MLS and single level data communications between nodes and MLS data communications between elements within a node. The system will be designed to use DoD standard protocols (i.e., IP, TCP, UDP, Telnet, SMTP, and FTP). It will be possible to upgrade the system to the emerging OSI protocol standards (i.e., X.25, IP, TP-4, X.400 Mail Services, File Transfer, Access, and Management (FTAM), and Virtual Terminal Protocol (VTP)). At that time, the system should be compatible with the ISO 7498 security working group efforts and the U.S. Government OSI Profile (GOSIP). For multilevel data exchange, the system will enforce mandatory and discretionary access controls, identification and authentication of communicating entities, and auditing of security events. It is desired that the system support DIA standards for DoDIIS Network Secure Information Exchange (DNSIX) for the secure transfer of information between systems. Tools will be provided for the management of network resources.

User Interface. The system will provide a graphical user interface based on the X Window/MOTIF standards. It is desirable that this system be based on a Trusted kernel and allow for the simultaneous display of data from multiple sessions, potentially at different sensitivity levels, on the workstation.

Hardcopy Output. The system will support both printers and pen plotter hardcopy output devices. It will be possible to output information at all sensitivity levels supported by the system to these devices. All output will be labelled at the top and bottom of each page in accordance with DoD regulations to reflect the maximum sensitivity level of information contained in the document.

Untrusted Applications. The system will support a variety of COTS and other application software designed to operate in conjunction with a POSIX/Unix compatible OS, SQL compatible database server, and X Window user interface server. This will consist of a COTS wordprocessor, COTS spreadsheet, COTS presentation graphics, an applications control executive, and on-line training programs. These applications will run as single level applications and contain no Trusted code.

Trusted Applications. The system will support developmental Trusted applications designed as extensions to the primary Trusted Computing Base (TCB) provided by the Trusted OS. This software will enforce specific aspects of the system security policy which are unique to the IAS application (see Section 3.9.2). They will provide extended Trusted Computing Base (TCB) functionality consistent with the concept of a partitioned TCB as defined in the NCSC-TG-021, Trusted Database Management System Interpretation.

Administration. The system will support a consistent, menu driven, interface for access to required administrative functions (security and non-security relevant). In accordance with the principle of least privilege, the system will provide a clear separation between security and non-security relevant functions.

Auditing. The system will support auditing of all security relevant events in accordance with DoD 5200.28-STD. It will be possible to select the type of audit information collected and establish administrative alarm thresholds for suspicious activities. It will be possible to archive audit data onto tertiary storage media. Tools will be provided for the analysis and review of audit data.

Diagnostics. Diagnostic software shall contain hardware diagnostic programs compatible with the requirements for FMF End User Computing Equipment (EUCE). Diagnostics to allow verification of security critical elements will be provided.

Training. The system will provide embedded training support.

3.2 CHARACTERISTICS

The MLS-IAS shall provide a MLS data processing environment in support of the G-2/S-2 staff. It shall provide the capability to input, store, retrieve, process, and disseminate data at multiple sensitivity levels. The system will support data integrity mechanisms to insure the correctness and consistency of data processed by the system. Data in the system will be protected from compromise in accordance with DoD security policy requirements and standard USMC intelligence operating procedures. This will include enforcement of both Mandatory Access Controls (MAC) and Discretionary Access Controls (DAC), positive identification and authentication of system users, maintenance of unambiguous sensitivity labels for all data, auditing of security relevant events, and enforcement of the concept of least privilege (see Section 3.3.9).

Functions supported by the three system configurations will include:

Functions	MEF/MEB	Intermediate	Single Workstation
Standardized Message Handling	X	X	X
Electronic Mail	X	X	
MLS Database Management	X	X	X
MLS File Management	X	X	X
Preparation of Textual Reports/Plans	X	X	X
Preparation of Graphical Reports	X	X	X
Display/Modification of Images	X	X	
Display/Modification of Maps &	X	X	

Overlays	X	X	
Intelligence Analysis	X	X	X
Intelligence Fusion	X	X	X
Collection Management	X	X	X
MLS Communications	X	X	X
Single Level Communications	X	X	X
System Administration	X	X	X
System Diagnostics	X	X	X

3.2.1 PERFORMANCE CHARACTERISTICS

3.2.1.1 OPERATING MODES

The MLS-IAS shall be capable of being operated in a battlefield, garrison, or shipboard environment. It shall be possible to flexibly tailor the complement of equipment to meet operational contingencies without compromising the inherent security and integrity provided by the system. When operating the MEF/MEB, Intermediate, or Single Workstation MLS-IAS system with a reduced complement of equipment, the system shall exhibit a graceful degradation in supported capabilities.

3.2.1.2 SYSTEM CAPABILITIES

A pictorial of the major IAS data flows is provided in Figure 3.2-1. As indicated, the system supports multiple sources of intelligence data which are input to the system via tactical communication channels. This data is received and processed to support the production of immediate and future intelligence products. The IAS supports an integrated Data Management System (DBMS) which may contain information spanning a range of sensitivities. This DBMS provides the primary data storage for the IDB and other intelligence databases as well storage of local "working" data for the IAS analysts who require efficient and flexible retrieval mechanisms. This data is utilized by the analysts for maintenance of an up-to-date situational assessment, in support of the generation of intelligence products for dissemination to operational elements of the MAGTF, and generation of collection requirements for supporting sensor systems. In support of these functions, the system must provide generation of reports, updates to external databases and preparation of military messages.

These basic requirements can be discussed in terms of four principal system functions. These include:

- Message management
- Database management
- Data fusion
- Collection management.

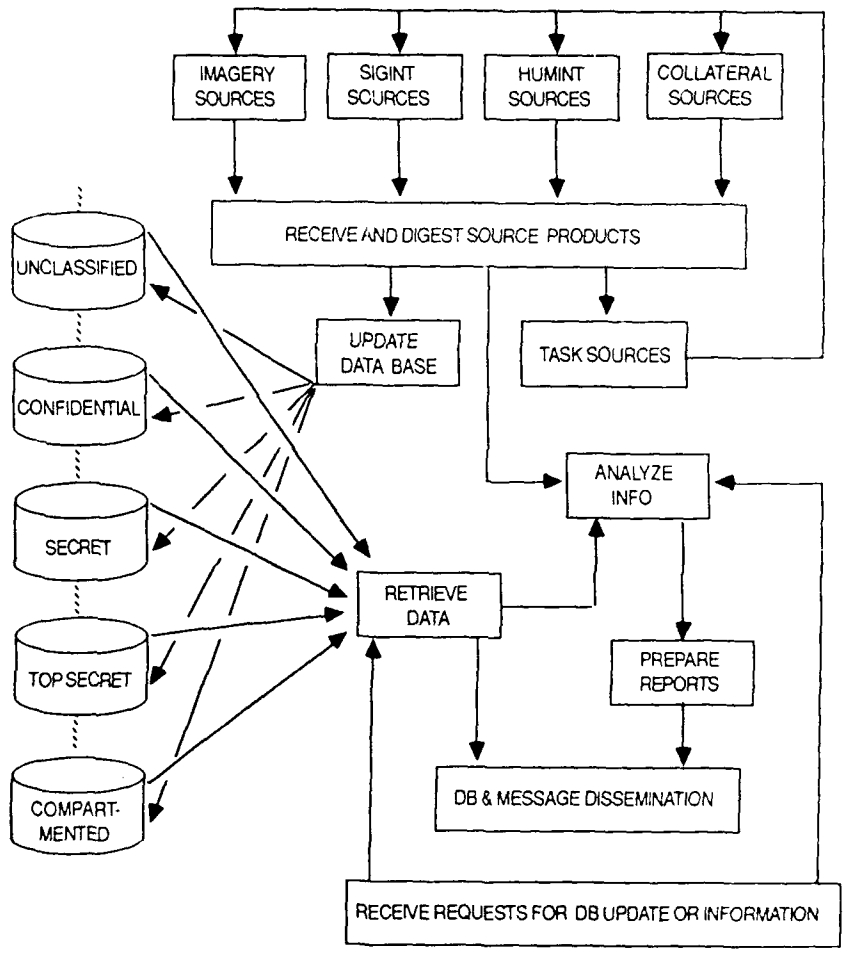

Figure 3.2-1. IAS Major Data Flows

Message management supports the external interface to other systems via formatted military messages. The IAS supports multiple message formats for the exchange of textual information and imagery. The database supports the efficient and flexible storage and retrieval of data within the system. This includes extracts from the IDB and other intelligence databases as well as internal data generated as intermediate

products in the analysis function. Data fusion represents the primary analysis, correlation, and interpretation process within the system required to generate intelligence products for use by the MAGTF operational components. Finally, collection management provides direction and tasking of supporting sensors and other collection assets to meet identified intelligence gaps. These functional elements are discussed in the subsequent paragraphs and their critical implications for operation in a multilevel secure environment are identified.

3.2.1.3 MESSAGE MANAGEMENT

The MLS-IAS will provide handling of standard military messages. The system will support, as a minimum, United States Message Text Format (USMTF) and Marine Tactical Systems (MTS) formatted messages, Position Location Information (PLI) and National Imagery Transmission Format (NITF). Incoming and outgoing messages may span the full range of data sensitivity supported by the MLS-IAS. It is desired that the multilevel nature of formatted military messages be recognized to allow the automated extraction of information with low sensitivity (e.g. source, destination, and Date-Time Group (DTG)) from a message with an overall high sensitivity classification.

The MEF/MEB and Intermediate MLS-IAS are required to provide the following basic message handling functions:

- Primary storage of incoming and outgoing messages
- Logging of messages into a journal log
- Printing of messages
- Logging of message content into journal file
- Manual creation and editing of messages
- Automatic distribution based on profiling
- Manual redistribution by watch officer and analyst
- Secondary storage on removable magnetic media
- Message retrieval based on DTG and precedence
- Retrieval based on DTG, body text, subject
- Assignment of default parameters when uninterpretable or missing data is present.

Within the Single Workstation MLS-IAS all of these functions will be supported except:

- Automatic printing of journal log entries
- Automatic distribution
- Secondary storage to removable magnetic media

In managing message traffic, the functions which must be performed can be broken down as depicted in Figure 3.2-2. The first function is the incoming message

distribution function. This is responsible for insuring the proper distribution for incoming messages and for invoking the appropriate communications handlers for outgoing messages. All messages handled by the message distribution function will have an associated sensitivity. For incoming messages this will be based on the source and input communications channel. For outgoing messages, sensitivity will be based on internally maintained information labelling of the MLS-IAS.

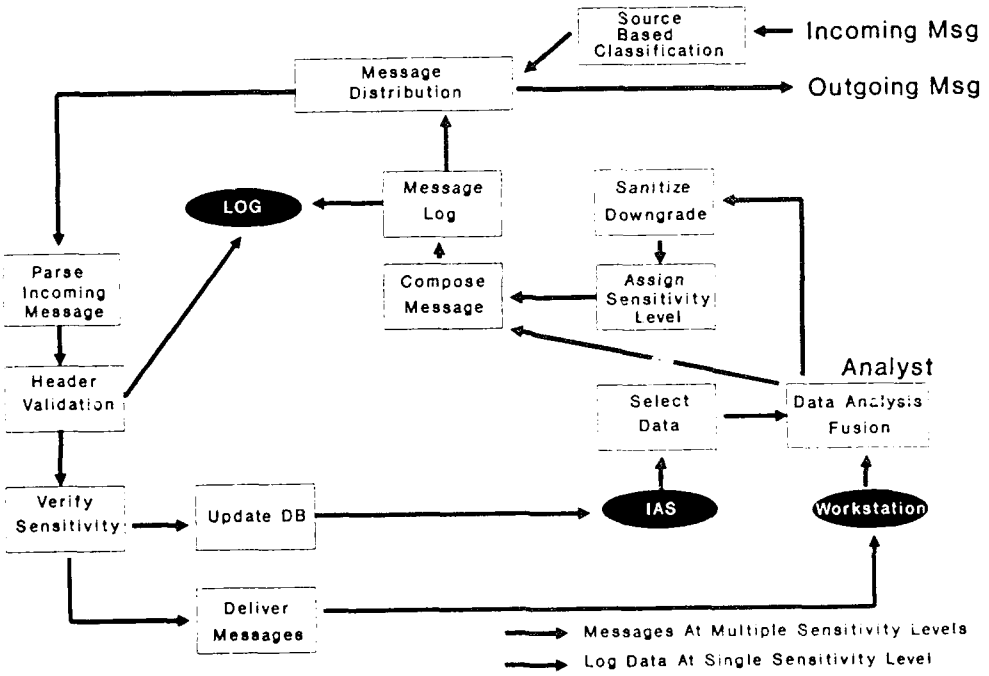

Figure 3.2-2. Message Management Operations

For incoming messages, the next actions are to parse the incoming message, breaking it into its constituent parts (header, body, trailer) and translating any encoded bit fields into their human readable equivalent. It is then possible to validate the header information (source, addressee list, DTG, etc.) This information can be used to support automated logging/journaling functions as discussed below. The message sensitivity can also be validated, generally by a human operator, and adjusted as required. The message can be delivered to the appropriate entities within the MLS-IAS. For messages containing database updates, this could generate an automated update request. For other messages, they would be distributed to appropriate analysts based on the list of addressees or on message profiling. This information is then available to support the analysts.

Outgoing messages must first be composed by an analyst within the system. The analyst can make use of available data (see paragraph 3.2.1.5, Data Fusion) in preparing such messages. If the source material is at the level of the new message, it can sent directly to the message composition/formatting function. If the analyst is extracting (sanitizing) data from highly sensitive source material, then a downgrading and sensitivity level assignment function must occur. After message composition, the message header is assembled with appropriate security sensitivity, annotated, and the message is sent to the outgoing distribution queue for logging and release.

Message logging and journaling operations will be conducted for all message traffic coming into and flowing out of IAS. Figure 3.2-3 depicts the logging and journaling function. The logging function is differentiated from the journaling function in that message logging is required by each workstation so that an audit of all message origination may be conducted. The log contains only minimal information required to identify the message. Once logged, the message can then be assigned to the journaling function which will add specific date and time of release fields, post message header information to the journal file, and allow addition of comments by authorized individuals to further identify specific attributes of the message or operational impacts. It is recognized that much of the basic journal information can be extracted from the message source and a prototype journal entry constructed. An authorized operator can then edit the journal entries to provide any required comments. It should be possible to retrieve or print all log and journal entries.

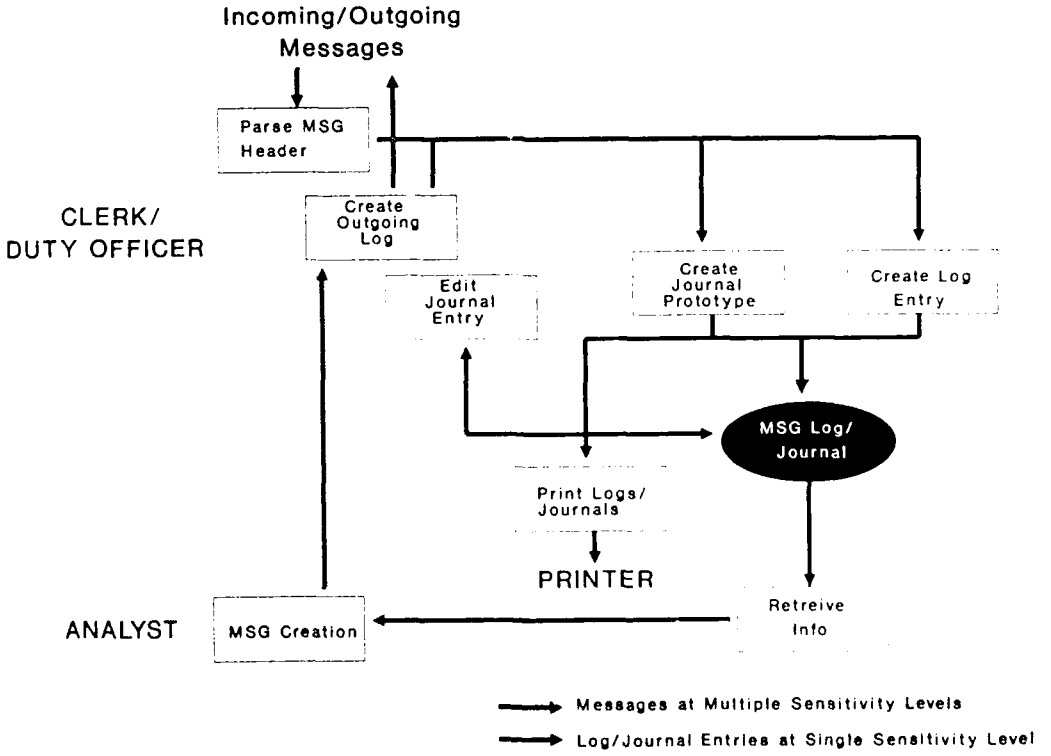

Figure 3.2-3. IAS Message Logging and Journaling Operation

Message traffic will span the full range of information sensitivities supported by the systems. However, it is desired that the message log file be maintained at a single low sensitivity level, which reflects the type of information maintained in the log, to simplify its maintenance and review. Similarly, the journal will generally contain information which is of more limited sensitivity than the source messages. The classification of the journal should reflect the sensitivity of the included information. This requires that we properly sanitize and downgrade information extracted from the source message traffic.

Message release operations within the MLS-IAS are supported by a series of message handlers, each optimized for a specific message protocol. A schematic of the message release flow is shown in Figure 3.2-4. Following message composition, it is generally required that validation of message source sensitivity be performed. This provides a check to insure that highly sensitivity information is not inadvertently released by the system. Should an invalid sensitivity level be detected, the message can be returned to an analyst for rework or modification. Messages leaving the system are physically separated by sensitivity level to insure that they are transmitted using authorized communications links with appropriate link encryption applied.

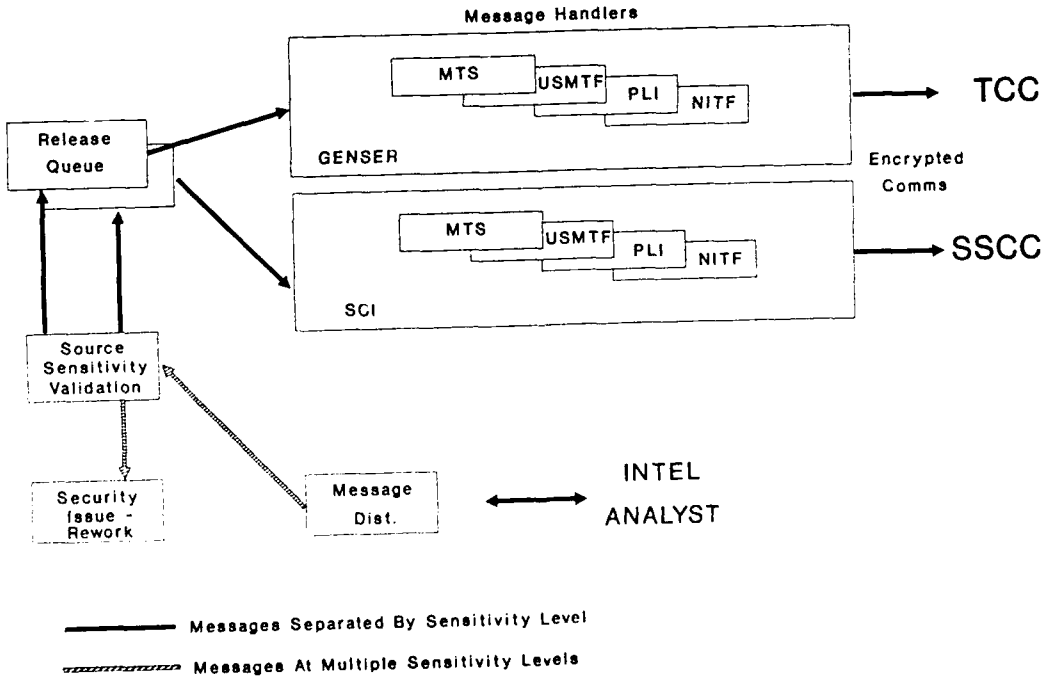

Figure 3.2-4. Message Release Operations

3.2.1.4 DATABASE OPERATIONS

The MSL-IAS will support multiple databases. Within the MEF/MEB and Intermediate nodes the system will support a centralized Marine Corps Tailored Database (MCTDB). This will be based on subsets of the Navy Integrated Data Base (NIDB) produced by the Fleet Intelligence Center. The NIDB consists of a combination of the DIA Integrated Data Base (IDB), Naval Warfare Tactical Data Base (NWTDB), amphibious files, merchant marine files, wreck files, and Characteristic and Performance (C&P) data. This database will contain multilevel data. The system must be capable of bulk loading pertinent segments of this database and updating the database using the DoD standard IDB Transaction Format (IDBTF). Other centralized databases will support situation assessment, Order Of Battle (OOB) information, weather, terrain, etc. The system will also support local databases which directly support the needs of individual analysts. This will include items such as workbooks, journals, logs, and messages. These databases should provide a set of uniform mechanisms for the storage, retrieval, and modification of textual, graphical, and imagery data.

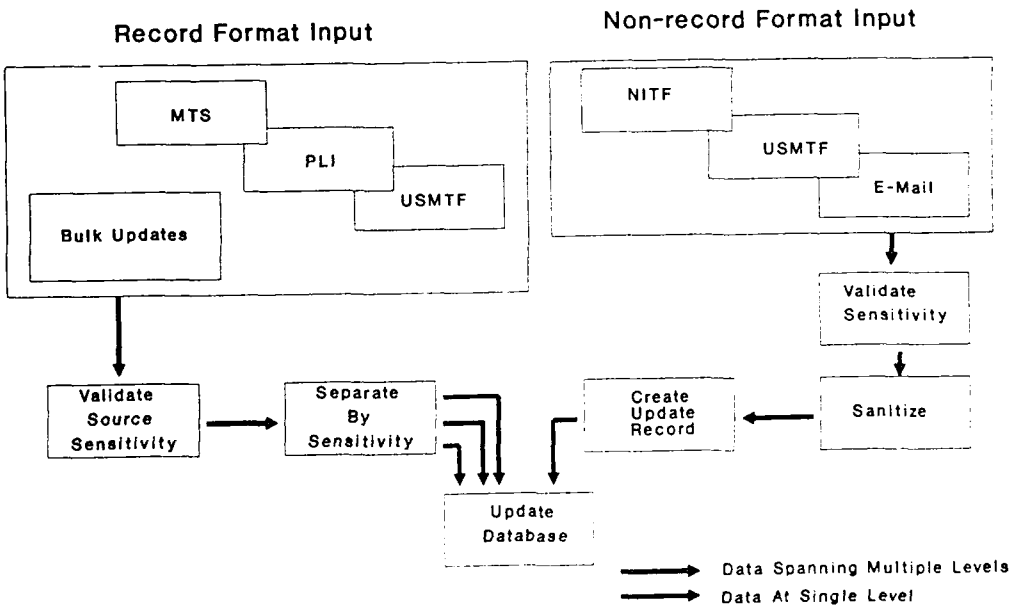

Figure 3.2-5. Database Update Operations

A key requirement will be the initial loading and maintenance of the centralized databases. These are expected to be of large size which will make manual entry or human input validation impractical. The approach to database update operations is shown in Figure 3.2-5. On the left hand side is shown the processing sequence for

inputs which are in a standardized database record format such as the IDBTF is shown. These may be input via archival storage devices (tape, disk) or encoded in either MTS or USMTF formats. The former will be the primary format used within the MAGTF while the latter will be used for interaction with elements external to the MAGTF. These records will contain adequate information to allow automated interpretation of data sensitivity values and conversion to internal MLS-IAS formats. Once converted, MAC within the MLS-IAS can enforce a logical separation of the data by sensitivity level and perform the automated update operation.

The other class of data which can update the IAS databases are messages which are not encoded in a recognized database record format. These messages must be manually parsed and a determination of the database update requirements made. This operation would be required for handling free form textual information and imagery. It may be necessary to extract and sanitize information in such messages prior to generating a database update. In this case, the appropriate sensitivity level for the update information must be determined and a sensitivity level assigned.

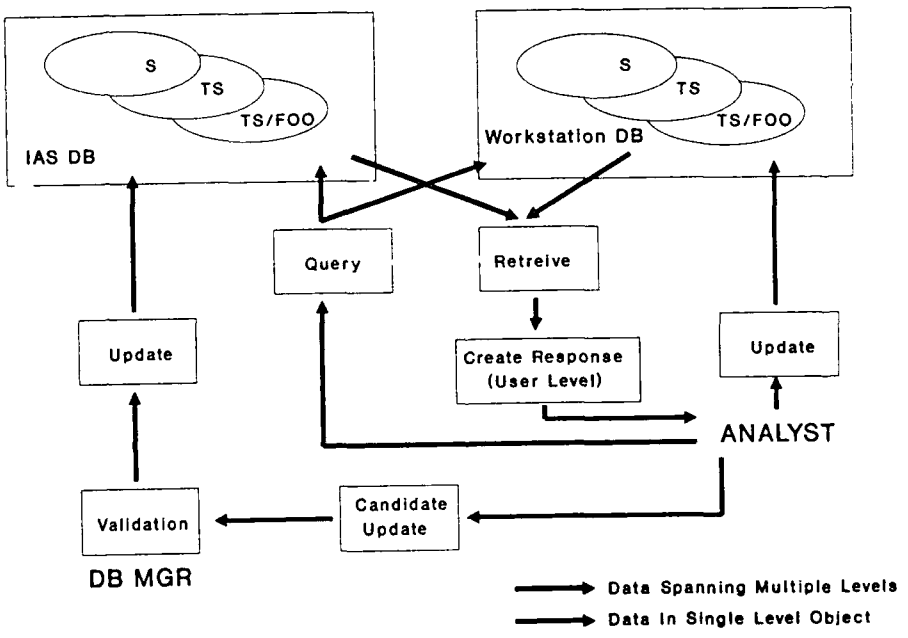

Figure 3.2-6. Internal Database Operations

The internal operations on the MCTDB and local databases are depicted in Figure 3.2-6. As shown, it is anticipated that these will generally be multilevel databases potentially containing a range of GENSER and SCI data. In accessing database

information, an analyst, working at a specific clearance level, would generate a query to the appropriate databases. The DBMS should return all information contained in the database which meets the query specifications and to which the user is authorized access. Authorization is determined by the user's clearance level and discretionary privileges established by the database owner. This information would be returned in a data object with a sensitivity level equal to the user's clearance level allowing him a full ability to read and modify the data.

The analyst can also generate updates to the databases. These updates are generated at the clearance level of the user and will contain data at only a single sensitivity level. For local databases, for which the user has update authority, the update would be immediately processed.

The analyst can also generate updates for the MCTDB and other centralized databases. This process would be ideally be fully automated; however, these databases represent a knowledge base which must be up to date, consistent, and have high integrity. As such, the database manager may chose to validate such updates and ensure that proper sensitivity validation occurs prior to executing the update. The system should support a manual review and validation function selectable at the discretion of the database manager.

3.2.1.5 DATA FUSION

Intelligence data fusion is a primary information processing function within the IAS. This process is supported by the system message management and database capabilities. Key elements in the data fusion process are shown in Figure 3.2-7. Data fusion drives the system to provide flexible and efficient handling capabilities of multilevel data. This includes both textual material as well as electronic maps, overlays, graphics, and imagery. The fusion process brings data together spanning the full range of sensitivity levels within the system. As such, efficient means to allow user display and interaction with information at multiple levels, such as provided by a multilevel windowed user interface, will be required.

The fusion process consists of correlation, analysis, and interpretation of available data. To aid in this process, the analyst will have the ability to maintain a local workbook which reflects intermediate results in this process. The workbook must support the storage and retrieval of multilevel data. We note that during the fusion process, aggregates of data are constructed and manipulated into new forms to allow its effective presentation. This aggregation process introduces security concerns in that the sensitivity level of such products may exceed that of the source material. This requires a capability to support man-in-loop procedures to validate data sensitivity.

The other result of the data fusion process is sanitized intelligence products. These represent data subsets, inferences, and data summaries based on the full range of

source material. To allow the dissemination of these products to the operational elements of the MAGTF, it must be sanitized and downgraded to the GENSER level. The system must support efficient tools for extracting data of low sensitivity for sources containing highly sensitive data, integrating such data, and assigning an appropriate sensitivity level to this data. Such products can then be used as the source material for preparation of military messages and/or updates to the IAS and external databases.

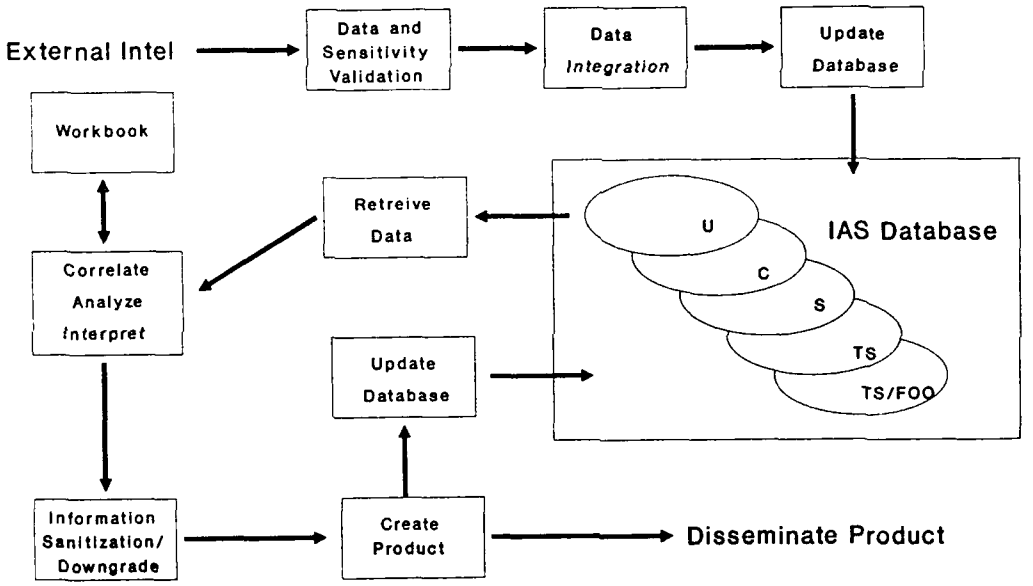

Figure 3.2-7. Intelligence Data Fusion

As an integral part of the fusion process, the system should provide efficient and flexible mechanisms for liaison and coordination between the analysts. An electronic mail system (E-mail) capable of supporting communications between all users of the system provides the necessary capabilities. This system should support the interchange of textual, graphical, and image data maintained in the system.

It is desired that the E-mail system provide a single point interface to all messaging capabilities within the system. In this manner, the E-mail application would provide consistent support to the analyst in terms of preparing and disseminating internal E-mail and military messages to external MAGTF elements. This system should make use of the system DBMS to allow the efficient storage and retrieval of multilevel

data. As a practical matter, the system should maintain a per-user log of all messages received by a user, at the lowest sensitivity level authorized for the user. This will allow a user to review arriving message traffic independent of the clearance level at which he is presently operating.

3.2.1.6 COLLECTION MANAGEMENT

Tactical collection management is a key element in the intelligence process, providing direction to the available collection resources on the critical data requirements of the MAGTF. The basic elements of the collection management process are indicated in Figure 3.2-8. This procedure supports the tasking of multiple sensitivity sources with collection requirements for the provisioning of intelligence data with the MLS-IAS. The key security aspect of tactical collection management are associated with the development and dissemination of collection tasking, or requests, to specific systems. The capabilities of these systems are classified at various sensitivity levels and the tasking messages may span a number of sensitivity levels.

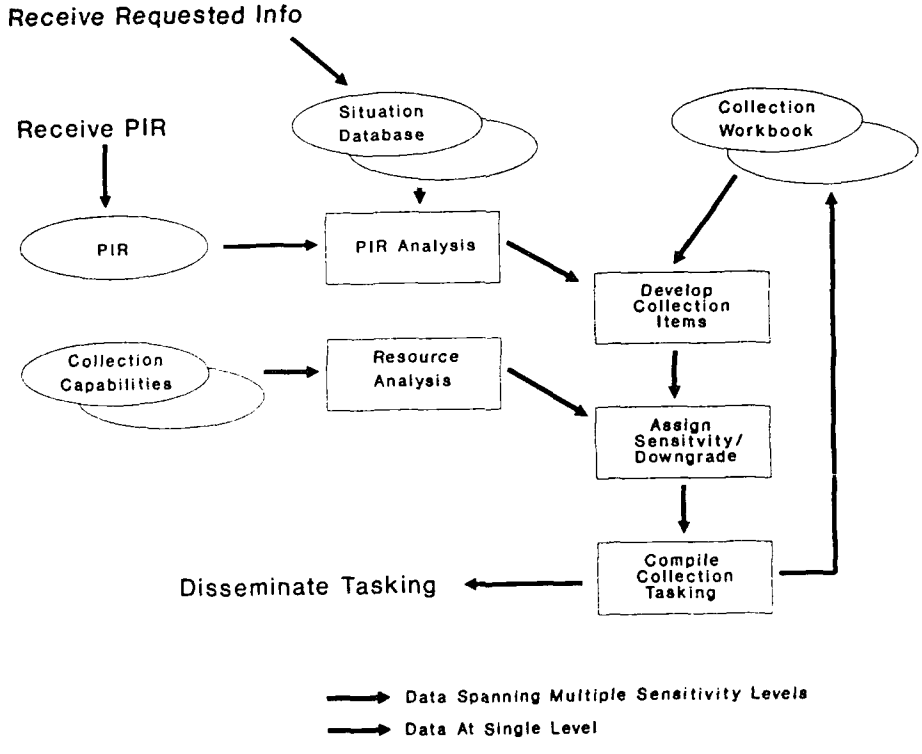

Figure 3.2-8. Tactical Collection Management

The key to collection management is the analyst's understanding of Priority Information Requirements (PIR). These requirements are stated by the consumers of the IAS intelligence product. PIR are analyzed in light of known information about the intelligence situation, which may span information at multiple sensitivity levels. New collection items are then generated to fill gaps in intelligence knowledge and to satisfy specific PIR or Essential Elements of Information (EEI). Through consideration of the desired collection items and the available sensor, or system, collection capabilities the analyst can generate a tasking message directed to the appropriate system. Many times technical collection parameters must be included in the tasking message, making it highly sensitive. Alternatively, it may be desirable to generate tasking which excludes highly classified system parameters utilized during analysis. In this case, the system should support efficient mechanisms to allow the analyst to sanitize the source data to generate a lower sensitivity message.

As part of the collection management process, the analyst will maintain a local workbook which reflects historical information on collection items and tasking. This may contain information at multiple sensitivity levels. Such a workbook should be integrated into the system DBMS capabilities.

3.2.1.7 INFORMATION SENSITIVITY VALIDATION

Facilities will be provided to allow the SysAdmin or other designated users of the MLS-IAS to review and validate the sensitivity of data imported into the system. This must occur prior to the data becoming generally accessible within the system. The user will be able to upgrade the sensitivity label associated with the data to any level within the authorized range for the user. This operation will require direct user to TCB communication via a Trusted Path.

The MLS-IAS will also provide a means of securely sanitizing and downgrading data objects within the system. It is desired that this be supported by a family of semi-automated tools which minimize required user interaction and eliminates the need to rekey information. As a minimum, these tools should support USMTF and MTS formatted messages, ASCII text files, and graphics data. These tools will assist the user in selectively extracting/editing data from a source document/file, displaying the information in a canonical format, and specifying a new data object at the proper sensitivity level to hold the sanitized data. The canonical format will provide a visual representation of all control information associated with the data which would not normally appear, but which controls data formatting and display. This will limit the potential for inadvertent information compromise. Validation of the true sensitivity of the target data will be the responsibility of the user. The data sensitivity may be established at any level which lies within the authorized minimum and maximum range for the user. These tools will require Trusted Path operation to insure direct user-TCB interaction.

3.2.1.8 OTHER APPLICATIONS

The MLS-IAS shall support a variety of applications necessary to allow the G-2/S-2 staff to perform their mission in a flexible and efficient manner. These applications will be identical to those in use on the IAS and other developmental systems. They must be designed to operate in an environment which supports:

- POSIX compatible OS
- X Window R11/MOTIF user interface
- SQL RDBMS
- POSIX standard network interface

These applications will run on the MLS-IAS, at the sensitivity level associated with the user session which invokes them, with minimal modifications. Applications include:

- Wordprocessing
- Spreadsheets
- Presentation graphics
- Raster/vector graphics display and modification (maps and overlays)
- Bitmap image display and modification (photos)
- Data analysis tools and decision aids

3.2.1.9 SYSTEM SOFTWARE CAPABILITIES

The MLS-IAS system software will be consistent with the requirements established for the IAS. It will provide additional functions and capabilities as required to provide multilevel secure operation in accordance with DoD regulations. Security relevant requirements for this software are summarized in the subsequent paragraphs.

3.2.1.9.1 Operating System

The MLS-IAS shall use a multitasking, multiuser Trusted Unix Operating System compliant with the IEEE 1003.1 POSIX standard. It will provide security functionality consistent with the B2 class as defined in DoD 5200.28-STD. The OS will be capable of running on all processors in all configurations of the system. It will provide process management, resource management, file system management, external device drivers, and distributed processing support. The OS will support a graphical user interface based on X Window/MOTIF.

Process Management. The OS will control the sequencing of all system processes, both internal and external to the TCB. For processes external to the TCB, a clearance level and the user on whose behalf the process is operating will be

maintained. Means of establishing relative priorities between processes will be provided.

Resource Management. Access to the hardware resources shall be through the OS applications interface. The OS will enforce MAC and DAC in determining the access rights of entities external to the TCB to hardware resources.

Inter-Process Communications (IPC). The OS will support a flexible set of IPC mechanisms as defined by the POSIX standard. Access to IPC channels will be controlled in accordance with the system security policy. The system will support IPC between processors within an MLS-IAS node. This will include support for remote procedure calls and inter-process message mechanisms required to support distributed client-server processing. All IPC mechanisms will enforce both MAC and DAC in accordance with the system security policy to protect against information compromise.

Device Drivers. The system will support installable device drivers to allow a wide range of peripheral devices to be supported. Access to device drivers will be controlled in accordance with the system security policy. Modification of the system device drivers will be restricted to the SysAdmin.

File Management Services. The MLS-IAS OS will support a multilevel file system(s). This may include a number of independent file systems mapped to multiple physical storage media. It will be possible to selectively install each physical device and to selectively mount and unmount the file system associated with them. The system will support remote file access and file sharing between processors within an MLS-IAS node using the NFS protocol.

The file system will be tree-structured with hierarchical directories containing a combination of files and sub-directories. Directories will be multilevel and capable of containing information spanning the range of sensitivities supported by the system. Files within the system will have a single sensitivity level associated with them which reflects the sensitivity of the data within the file. Both files and directories will have associated Access Control Lists (ACLs) which can be used to restrict access on a named individual basis.

The system will support the following functions, with access controlled in accordance with the system security policy, as a minimum:

- Create a directory
- Read the contents of a directory
- Delete a directory
- Create a file
- Read a file
- Write to a file

- Delete a file
- Modify an ACL.

It will be possible for an unauthorized user to alter the sensitivity label associated with a directory or file through invocation of a privileged operation as discussed in paragraph 3.2.1.7.

Graphical User Interface. The system will use the X Window/MOTIF software as the standard user interface. It is desirable that the X Window server be Trusted to allow the simultaneous display of output from multiple processes acting at independent sensitivity levels within the authorized range for the user. This should meet the requirements of the DIA CMW program. Operation at the B2 certification is desired.

A typical display screen would appear as shown in Figure 3.2-9. Each window will provide an indication of the maximum sensitivity level of all data which may be displayed in the window. In addition, floating information labels which reflect the sensitivity of the source data used in building the displayed data may be provided (as defined for the CMW program). These floating labels are advisory only and are provided as an aid to the user. A positive indication of the sensitivity level associated with user input is required.

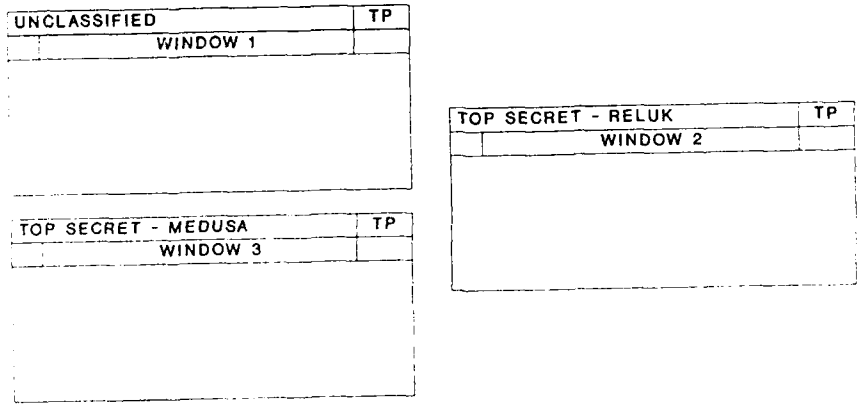

Figure 3.2-9. Multilevel Windowed User Interface

For operations which require direct user interaction with the TCB, the user interface will provide a positive indication that a Trusted Path exists. Such operations include log-on/log-off, invocation of a new user session at a new sensitivity level, and performance of all security critical administrative actions.

3.2.1.9.2 Database Management

The RDBMS will provide for secure storage, retrieval, modification of multilevel data within the MLS-IAS. It will serve as the primary repository for data within the system and it is desirable that other subsystems utilize the data management facilities of the RDBMS to the maximum extent in storing intelligence information.

It is desired that a single Trusted RDBMS product provide the required centralized IAS database server required to support the IDB, other large, widely used databases, and the local databases at each workstation to support the individual analyst. Both databases should provide a consistent interface to user applications programs based on the client-server processing model. Basic features of the RDBMS will include:

- Support for the relational data model
- SQL based Data Definition Language (DDL)and Data Manipulation Language (DML) Interface
- Support for a menu driven interaction with the database and embedded applications
- On-line context sensitive help
- Applications generator
- Ability to create custom screens and reports
- Ability to generate queries which span multiple databases and tables within a database
- Support for compiled procedures and event driven triggers
- Support for standard numeric, characters and date data types plus support for variable sized text and binary data
- Support for data views to allow logical views of the database to be generated in support of specific users
- Input validation and integrity checking
- Consistency and recovery tools

It is desired that the RDBMS run as an application on top of the selected Trusted OS to avoid the need for a dedicated database server hardware. The RDBMS should make extensive use of the OS security databases to avoid the need to define unique sensitivity levels or user databases for use by the RDBMS. The RDBMS will provide the following security features:

- Sensitivity labelling and MAC enforcement to at least the tuple (record) level.
- Ability to restrict the range of data sensitivity allowed in a database

- Ability to return all information meeting a query specification which is dominated by the user's active clearance level
- Maintenance of ACLs and DAC enforcement at the Database level.
- DAC for all RDBMS database definition commands, interface programs, screen and report definition tools, and programming tools.
- Selective over-write/polyinstantiation capability when updating a record at a new sensitivity level
- Ability to archive/restore multilevel databases
- Selective auditing of security relevant events

An example of the anticipated RDBMS capabilities are depicted in Figure 3.2-10 for a user query operation. This shows a user process, operating at the Secret (S) level generating a database query. Assuming that the user has discretionary access to Database 'B', the Secret level query will be handled by the database query module which will optimize and execute it against the stored data. This process should retrieve all data whose sensitivity is dominated by the user process' clearance level. This data will be formatted, copied into a Secret level storage object which the user process can access.

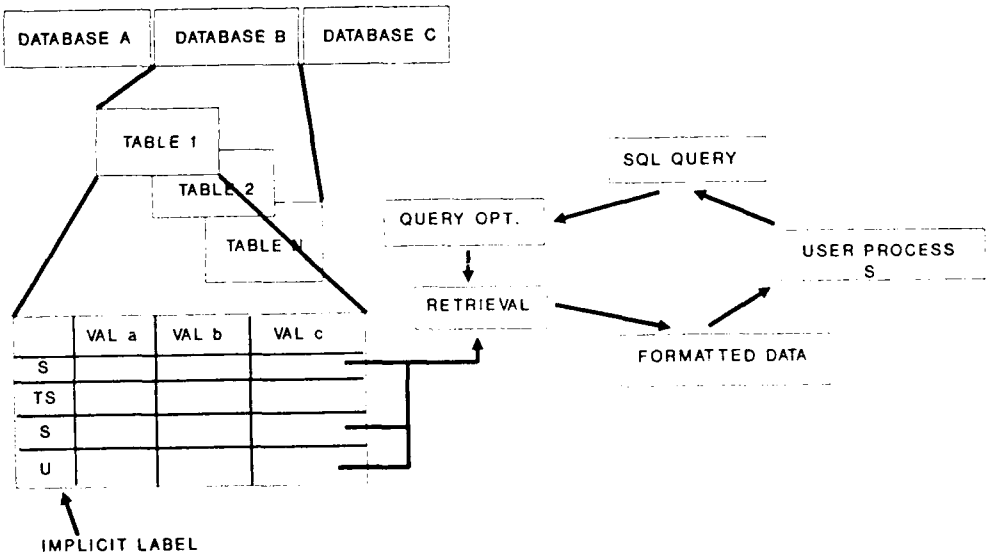

Figure 3.2-10. Database Query Operations

Other operations supported by the RDBMS would include:

Database Creation.Users will be able to create databases and define data tables, fields, integrity constraints, triggers, and ACLs. It will be possible to define the minimum and maximum sensitivity associated with the database.

Database Modification. The ability to modify the database definition will be restricted to the database owner (creator). This will include permission to delete the database.

Record Creation. All users with discretionary write access, operating at a clearance level within the sensitivity range specified for the database, will be able to add new records to the database. Record data will be entered at a single sensitivity level.

Record Modification. All users with discretionary read/write access, operating at a clearance level within the sensitivity range specified for the database, will be able to update and delete existing records. The new record will be written at the current clearance level associated with the user.

3.2.1.9.3 Network Software

The MEF/MEB and Intermediate MLS-IAS configurations will support multilevel data communications and the exchange of control information between host elements. A dedicated MLS LAN, to which only the MLS-IAS Trusted processing elements will be connected, will be utilized for this purpose. Interfaces to other LANs or communications systems will be via a secure communications gateway function provided in the MLS-IAS communications server. The MLS LAN will function as a multilevel device as identified in the DoD 5200.28-STD and the interface will meet all of the requirements for a MDIA (MAC, DAC, Identification, and Audit functions) device as specified in the Trusted Network Interpretation (TNI). This may be accomplished through a combination of host based protocol and network component mechanisms.

The applications interface to the LAN will be via the DoD standard protocols TCP/UDP or applications layer protocols such as FTP, SMTP, Telnet, and MLS-IAS message handlers (MTS, USMTF support). Both connection oriented and connectionless services will be supported. It is desired that the system be compatible with the DNSIX specification for secure network services.

It is desired that the network software be integrated with the Trusted OS and make use of its internal security databases. In addition, the Trusted network will support definition of network databases which define elements such as:

- Host node identification values
- Mapping from internal labels to Revised IP Security Option (RIPSO) compliant datagram labels
- Data sensitivity ranges supported by external systems
- Routing constraints

Access to these features will be restricted to a designated system administrator.

The network will be capable of restricting access between a host and all external entities in accordance with the system mandatory policy and on a named user basis on a discretionary basis. Other security features will include:

- Sensitivity labelling of all datagrams which reflects the clearance level associated with the originating process
- MAC enforcement on the delivery of all datagrams
- Ability to restrict the range of data sensitivity allowed on the network
- DAC enforcement for all sessions/datagrams
- Selective auditing al security relevant events

It is desired that the network also support the following services:

- Assurance that communications are addressed to a peer entity and that the source is the one claimed
- Protection of data/header fields from unauthorized modification
- Non-repudiation services to provide unforgeable proof of shipment and/or receipt of data
- Denial of Service protection against interruption of service due to external factors

3.2.1.9.4 AUDIT

The TCB will provide the capability to audit all security relevant events which occur within the system in accordance with the requirements of DoD 5200.28-STD. The SysAdmin will be able to selectively control the type of audit data collected, including the ability to disable auditing. The audit data will be written to a distinguished area within the multilevel file system which is only accessible to the SysAdmin or other designated individuals.

A set of tools will be provided for audit reduction and analysis. The tools should provide the capability to:

- Search for records based on time
- Search for records based on individual
- Search for records based on event type
- Provide summary information by individual and event type

- Allow archive storage of audit data
- Allow printing of selected audit records or summary data

3.2.1.9.5 ADMINISTRATIVE SOFTWARE

Administrative software will support all required administrative tasks, both security and non-security relevant. This will include:

Backup and Recovery. Provide selective archiving and restoration of information maintained in the file system.

File System Management. Provide creation, mounting, unmounting, and deletion of file systems. Utilities will also be available to aid in performing consistency checking and recovering from errors. The SysAdmin will be able to establish access privileges and sensitivity levels associated with a file system.

Auditing. Interface to the audit system in accordance with the functions identified previously.

Device Management. Install and de-install device drivers. Allow devices to be designated as single or multilevel devices and establish associated sensitivity levels(s) for a device.

Key Management. Load, assign, and clear cryptographic key variables utilized by internal encryption algorithms.

Security Databases. Establish the sensitivity level databases and the mapping of internal labels to human readable labels. Provide management of the user database to include creation, deleting, and altering the parameters associated with a user (clearance level, password, etc.).

System Purge. Allow selective purging of storage objects within the system to provide assured declassification of resources.

System Start-up/Shutdown. Allow system initialization and verification of secure operation. The SysAdmin will be able to shut-down the system on command. This will securely terminate all system processes and automatically log-off all users.

Database System Management. Allow establishing of authorization lists for database access, establishing sensitivity level restrictions for databases, and purging of database data. Provide tools to allow for the archiving, restoration, and bulk loading of databases.

Network Management. Support management of the LAN in terms of network configuration, host address specification, sensitivity level limits, and designation of

user access privileges. Also provide mechanisms to allow the LAN to be activated/de-activated upon command.

A more detailed description of security relevant administrative functionality can be found in paragraph 3.3.9.3.12.

3.2.1.9.6 DIAGNOSTIC SOFTWARE

The system will provide general purpose diagnostic software consistent with the requirements for the IAS. In addition, the system will provide diagnostic software capable of verifying the integrity of all system security mechanisms in accordance with the requirements of DoD 5200.28-STD.

3.2.1.9.7 TRAINING

The system will provide embedded training software in accordance with the requirements for the IAS.

3.2.1.10 HARDWARE CAPABILITIES

The general hardware capabilities of the MLS-IAS will be consistent with those specified for the IAS and the MCHS. Security relevant considerations are summarized in the subsequent paragraphs.

Workstations. The workstations employed in the MLS-IAS will be based on a standard vonNeumann architecture. The technology to secure advanced architectures (data driven processing, fine grained parallel architectures) is not sufficiently mature to support development of an MLS system incorporating such elements. The systems may employ symmetric multi-processing such as commonly supported by commercial Unix implementations.

Industry standard processors will be utilized to insure an adequate base of COTS Trusted components. This includes processors such as the 80X86 family, 680X0 family, SPARC, MIPS, etc. Memory management support capable of enforcing distinct logical address spaces for all system processes must be available. In addition to supporting the integrity of multitasking systems, such support is critical to the enforcement mechanisms employed by existing COTS TCBs.

The workstation will employ an industry standard bus architecture (VME, Multibus, etc.) to allow use of peripheral devices which are supported by COTS Trusted OS vendors.

Display Terminals. The system will provide high resolution graphics displays as the primary means of providing data to the user. This will be supported as a multilevel device.

Keyboards/Pointing Devices. The MLS-IAS shall support both keyboard and pointing device (mouse, trackball, etc.) for user input. The sensitivity of data input from these devices will be determined by the currently active user process awaiting input. During Trusted Path operations (e.g., log-on, changing sessions) the keyboard and pointing device will allow the user to communicate directly with the TCB.

Secondary Storage. The MLS-IAS will support removable and fixed read/write magnetic and optical disks for secondary storage. These devices will be multilevel and be accessible via mounting of the associated file system. It is preferred that these devices interface to the host system via a SCSI standard interface. Workstations will have a 200 MB magnetic disk as a minimum and the File/Database/Comm servers located at the MEF/MEB and Intermediate nodes will support multiple disks with a capacity of up to 12 GB.

CD-ROM. The MLS-IAS will support CD-ROM drives capable of reading disks in the High Sierra Group and ISO-9660 formats. It will be possible to mount the CD-ROM as a POSIX compatible file system. This file system will be designated as read only for all users on the system. To allow utilization of CD-ROM disks which do not contain embedded sensitivity labels consistent with the file system format utilized by the MLS-IAS, it will be possible to specify the CD-ROM file system as single level, with an implied sensitivity level for all contained directories and files designated by the SysAdmin.

Archival Storage. Each MLS-IAS node will provide archival storage of information using magnetic tape or disk (magnetic or optical) tertiary storage media. The selected magnetic tape and/or disk media should be consistent with the MCHS specified hardware. Potential options for magnetic tape media include Cartridge Tape; DAT tape; or 9-Track reel-to-reel tape. Potential disk media include high density floppy disks; removable hard disk cartridges; or writable optical disks.

The SysAdmin will be able to selectively enable each archive device on the system as either a single or multilevel device. Changing between the two modes will only be possible when the device is inactive. It is the responsibility of the SysAdmin to insure that storage media is changed as required and properly labelled with human readable sensitivity markings. All removable media must be controlled in accordance with DoD and USMC regulations for the protection of classified information.

The preferred data format to store MLS information is dependent upon evolving POSIX, MCASS and other standardization efforts. Until such standards are defined, it is desired that the MLS-IAS system support the POSIX Portable Archive Format ("pax") (includes support for Unix standard "tar" and "cpio" formats) for the storage of single level data. Archival storage of multilevel data may be done in a OS designated format.

Paper Tape. The MLS-IAS will support a paper tape read/punch as a single level device. This device will support both eight and five level tapes in accordance with the EIA-227-A standard. The sensitivity level associated with data read/written to the paper tape device will be selectable by the SysAdmin.

Hardcopy Output. The MLS-IAS shall support printer and pen plotter devices. These devices will be able to serially output information at the full range of data sensitivities supported by the system, or a sub-range specified by the SysAdmin. Such setting will only be modifiable when the hardcopy device is inactive. All data will be formatted and human readable sensitivity labels, which reflect the highest level of classification associated with the data file being printed, written to the top and bottom of each page. All hardcopy output must be controlled in accordance with DoD and USMC regulations for the protection of classified information.

The system will provide print spooling software which is capable of sequencing and prioritizing multiple hardcopy output requests in accordance with priorities defined by the SysAdmin.

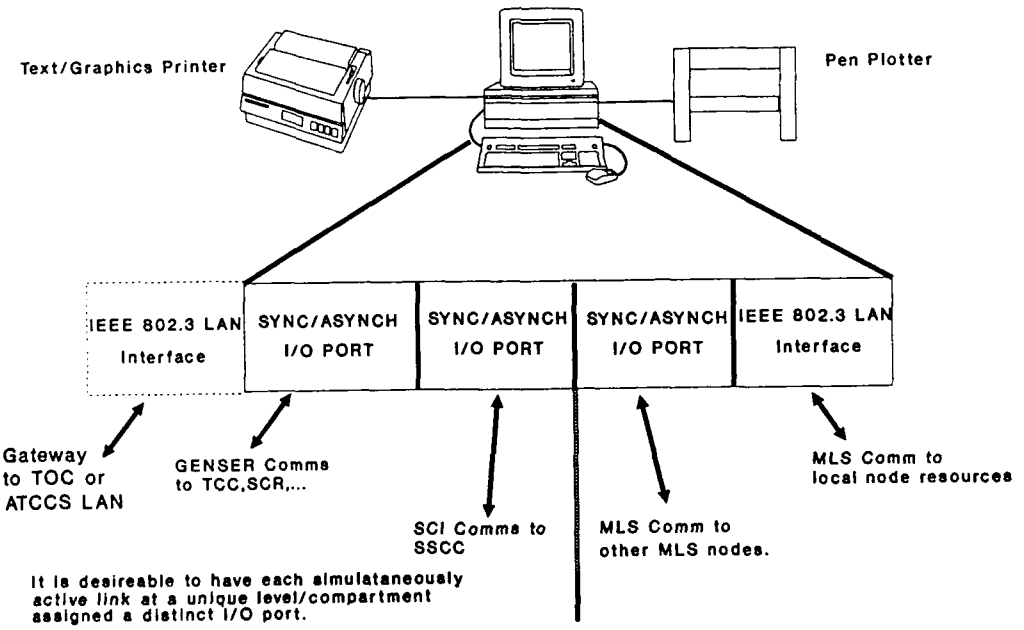

Figure 3.2-11. Multilevel Communications Channel Support

Communications. The MLS-IAS will support both single and multilevel external communications channels as indicated in Figure 3.2.11. Each host in the system will

support an IEEE 802.3 Ethernet interface as a multilevel device. In addition, it is desirable that the communications server at the MEF/MEB and Intermediate nodes be capable of supporting a second Ethernet interface as a single level device. This would be used to provide automated linkage to the TCO and/or ATACC LANs.

The LAN media will be physically protected from tampering, wire taps, and other active and passive attempts to hostile entities to capture, modify, or insert traffic on the LAN. Link level encryption will not be required to insure data confidentiality and logical separation of data at different sensitivity levels. End-to-end encryption may be employed as required to provide assured bindings between sensitivity labels and data and to insure data integrity. It will be possible to rapidly reconfigure the MLS-LAN to add or delete components.

The system will also support multiple synchronous/asynchronous serial I/O ports and Centronics-type parallel ports at each processor. It will be possible to configure each port as either a single or multilevel device.

3.2.1.11 SELF DESTRUCT

The MLS-IAS will incorporate a self-destruct means, with appropriate safety devices and safeguards, which will enable a single Marine to rapidly destroy both the data and the equipment to prevent it from falling into enemy hands. The degree of destruction required will be that which is sufficient to prevent the enemy from determining through exploitation activities the intelligence-related capabilities of the equipment.

3..2.1.12 TEMPEST

MLS-IAS system components will be TEMPEST approved, or approved for use within a limited physical exclusion zone, in accordance with NACSIM 5100A to protect against exploitation of electromagnetic emissions.

3.2.1.13 COMSEC

The MLS-IAS shall interface with approved COMSEC devices to provide link level encryption of digital communications. Such devices include the TSEC/KY-57/58, TSEC/KG-84, Embedded COMSEC for SINCGARS, STU-III, DSVT, and BLACKER.

3.2.2 SYSTEM CAPABILITY RELATIONSHIPS

The MLS-IAS system supports the management of military messages, data management, data fusion, and collection management as discussed in Paragraph 3.2.1. These functions are implemented in a manner consistent with multilevel secure operation capable of handling both GENSER and SCI data. These

capabilities are supported by a comprehensive set of security mechanisms built upon an integrated set of COMPUSEC, COMSEC, TEMPEST, and physical security elements as depicted in Figure 3.2.12.

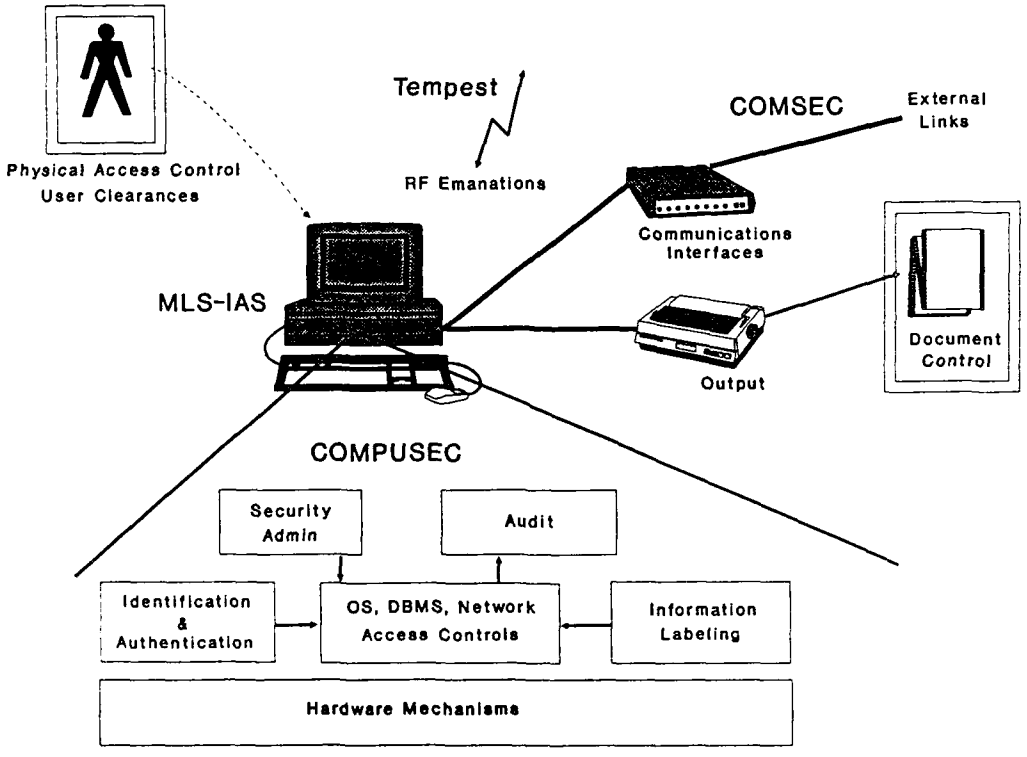

Figure 3.2.12. Relationship Between System Security Features

COMPUSEC. The COMPUSEC (Computer Security) mechanisms are compliant with B2 class protection as defined in DoD 5200.28-STD. These mechanisms are responsible for enforcing the logical separation of data by sensitivity level for all data processed by the system. They also control access to this data by users of the system in accordance with DoD policy. A set of diagnostic, audit, and administrative functions provide continued assurance of proper system operation.

Physical Security. Physical security provides control over access of individuals to the system hardware to prevent theft, tampering, and passive observation of system operation.

TEMPEST. The TEMPEST mechanisms protect the system from passive collection of radiated electromagnetic energy which could be used to determine system operation and data being processed.

COMSEC. COMSEC (Communications Security) insures that information transmitted over communications links external to the system can not be intercepted and the data being transmitted correctly interpreted.

3.2.3 SYSTEM EXTERNAL INTERFACE REQUIREMENTS

The MLS-IAS will support both GENSER and SCI communications. This will include support of communications at the MAGTF CE level with Commander Amphibious Task Force (CWATF) and other Amphibious Task Force (ATF) units; with other MAGIS components such as TERPES, JSIPS, TCAC, HUMINT and RECON sources, TPCS, TRSS; with TCO and ATACC; and with other IAS systems at different echelons/units within the MAGTF. The primary means of communications external to the MAGTF will be USMTF messages for textual material and NITF for imagery products until implementation of the DODIIS DTEP. Within the MAGTF, the MTS protocols are expected to be the primary format for textual messages. An overview of the required communications interfaces is presented in Figure 3.2-13.

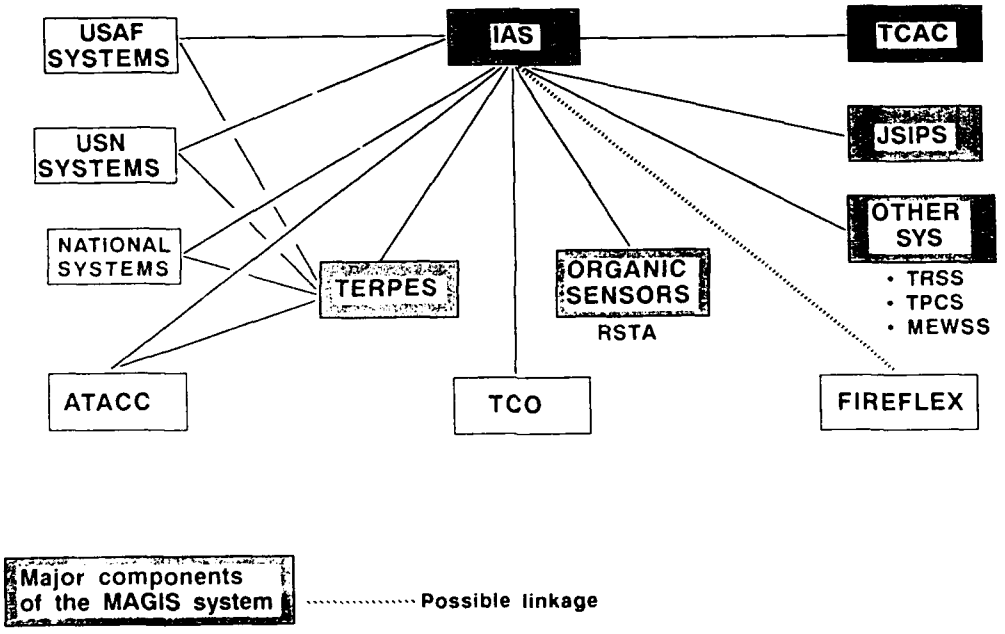

Figure 3.2-13. MLS-IAS Communications Interfaces

At the present time, all systems external to the MLS-IAS operate in a System High or Dedicated security mode. Hence, these interfaces are all operated at a single security level. This is expected to change in the future as multilevel operation is introduced into more components.

The primary communications means for the MLS-IAS textual message traffic are through the USMC digital communications backbone provided by the TCC and SSCC. The relationship between the MLS-IAS nodes and the TCC and SSCC elements is depicted in Figure 3.2-14. The TCC (Telecommunications Center) AN/MSC-63A(V)Y provides GENSER services and the SSCC (Special Security Communications Center) AN/MSC-63(V) supports communications at the SCI level. These capabilities are supplemented with wire-line, Single Channel HF/VHF/UHF Radio (SCR), Satellite Communications (SATCOM), and direct LAN-to-LAN connectivity.

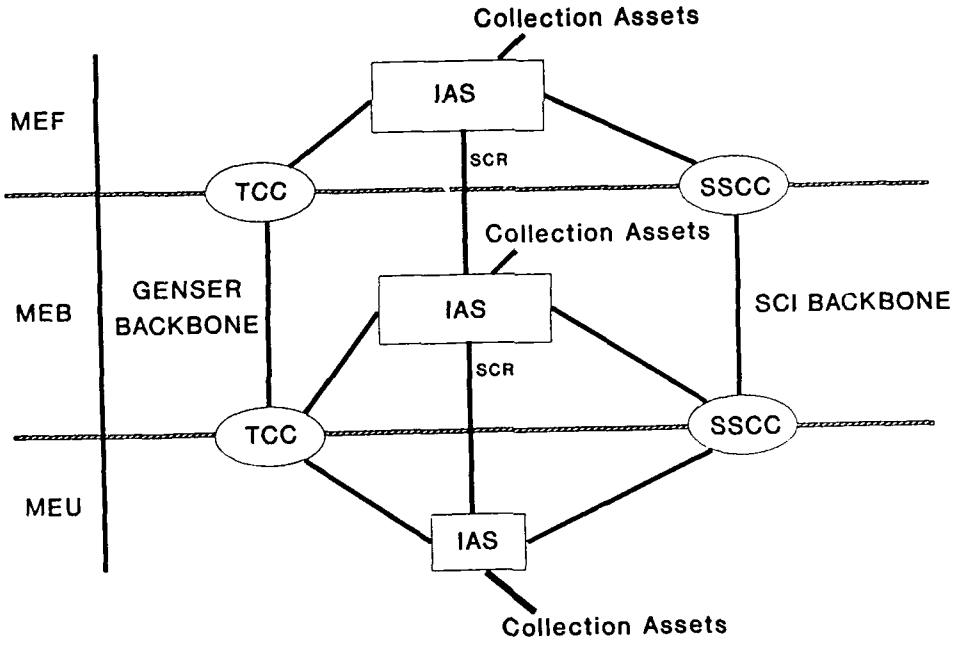

Figure 3.2-14. Interfaces to the Marine GENSER and SCI Backbone Communications

The interface requirement of each system which interfaces to MLS-IAS is briefly discussed in the following paragraphs:

TCO. This interface provides the primary link for dissemination of tactical intelligence to the commander at the various MAGTF CEs. This interface will be supported by a digital communications link. It is desired that the system support direct interface to the TCO LAN, SCR broadcast capability (MTS protocols), and switched backbone communications (MTS protocols).

ATACCS. This interface provides the primary link for dissemination of tactical intelligence to the commander at the Air Command Element (ACE). This interface will be a digital linkage and may be implemented by allowing the IAS to have terminal status on the ATACC LAN, by broadcast Marine Tactical System (MTS), or by switched backbone communications supporting (MTS).

TERPES. TERPES provides Electronic Warfare (EW) and Electronic Support Measures (ESM) information to the IAS. It is regarded as a subordinate system in the MAGIS hierarchy of system. Currently the system supports only GENSER communications. Planned upgrades will allow the system to pass SCI information.

JSIPS. The JSIPS provides both hardcopy imagery and textual messages to the IAS. The imagery transmission is supported by the National Imagery Transmission Format (NITF). Text messages are used to provide exploitation reports and general communications between systems. Interface is via switched backbone communications.

TCAC. The TCAC provides the primary interface for IAS into the organic SIGINT community. This interface will pass highly sensitive (SCI) information and will support both resource tasking and reporting.

JOINT/NATIONAL SYSTEM. The IAS will be required to interoperate with U. S. Navy intelligence systems while embarked with the Navy at sea. The IAS will be directly interoperable with the (1) Intelligence Support to Strike/Amphibious Forces (ISS/AF) systems (an intelligence system concept for the U.S. Navy) and (2) Tactical Flag Command Center (TFCC) systems, which support Naval combat operations and is in the definition/development stage. The IAS shall be capable of receiving intelligence information in a digital format from DODIIS agents via services tactical communications nets when the DODIIS Tactical Extension Program (DTEP) is fielded. Multilevel data communications will be supported using DNSIX. Prior to the fielding of the DTEP, the IAS will be capable of digital exchange of DODIIS data via magnetic tape.

TPCS. At the lower MAGTF levels (MEU), organic support is provided to tactical forces by the TPCS. When this capability is provided, the TPCS interfaces directly with the IAS. This interface will support the exchange of highly sensitive (SCI) information.

TRSS. The TRSS system will be organic to the Sensor Control and Management Platoon (SCAMP) and consists of a family of hand implaced or air delivered sensors. The TRSS outputs Sensor Reports (SENREP) that may be provided to the IAS by hard copy, magnetic disk, or digital communications.

RECON. The Force Reconnaissance Company (SRIG) and the Reconnaissance battalions will communicate using SCR and/or DCT type burst digital transmissions. The IAS will support existing DCT messages used for reporting RECON generated information.

OTHER INTEROPERABILITY REQUIREMENTS. The IAS is required to provide intelligence data base updates in an automated manner to USMC aircraft mission planning devices to include the Tactical Aircraft Mission Planning System (TAMPS) and Map Operation maintenance Station (MOMS). This requirement may be met by direct information feed from the IAS or indirectly via the ATACC.

3.2.4 PHYSICAL CHARACTERISTICS

The physical characteristics of the MLS-IAS components will conform to those for the selected MCHS hardware.

3.2.5 SYSTEM QUALITY FACTORS

The hardware and software design will emphasize simplicity in order to provide a high degree of reliability and maintainability. Components should essentially be able to be "snapped" in and out of position for quick repairs. This modular design will enable the user to make quick repairs in a combat environment without debugging the system "manually." There should also be a diagnostic capability for the system that tells the user which component is at fault. These diagnostic capabilities shall also provide a SysAdmin the capability to perform analysis of security controls and provide warnings for system security failure modes.

IAS configurations which include more than one workstation shall be capable of 24 hour per day battlefield operations in a degraded mode (i.e., at least one workstation operating). Single workstation configurations shall be capable of battlefield operation for 22 hours per day.

3.2.5.1 RELIABILITY FACTORS

Provisions will be included in the MLS-IAS to prevent loss of data, incorrect computation, loss of system security, or damage to equipment in the event of power system malfunction. Operational parameters to include MD, OMF, and MTBF will be consistent with those for the selected MCHS hardware.

3.2.5.2 MAINTAINABILITY

The MLS-IAS MTTR will be consistent with that for the MCHS selected hardware with the exception that 15 minutes will be allowed for verification of system integrity and proper operation of security mechanisms following any system hardware repair or modification.

3.2.5.3 AVAILABILITY

Availability of the MLS-IAS will be in accordance with that for the MCHS selected hardware.

3.2.6 ENVIRONMENTAL CONDITIONS

Environmental conditions for the MLS-IAS will be consistent with those for the existing IAS and the MCHS hardware when specified.

3.2.7 TRANSPORTABILITY

Transportability of the MEF/MEB, Intermediate, and Single Workstation elements of the MLS-IAS will be consistent with the existing IAS system and the MCHS hardware when specified.

3.2.8 FLEXIBILITY AND EXPANSION

The MLS-IAS will be employed by USMC intelligence sections throughout the world in both garrison and field deployments. In garrison, the system will be utilized as the G-2/S-2 desires. In operational employment, the MLS-IAS will be set up and employed in the unit's command and control facility (C2 FAC). When employed aboard ship, MLS-IAS equipment will be utilized in existing Joint Intelligence Center (JIC) spaces when possible. The IAS will be modular and reconfigurable in nature, thereby allowing the G-2/S-2 the flexibility to configure the system to meet situationally dictated operational requirements.

The MLS-IAS will provide flexibility through the use of a distributed operation concept. Within the MLS-IAS, workstations, servers, and peripheral devices within a given system node are connected via a multilevel secure LAN. Inter-node connectivity is provided by multilevel secure gateways capable of communication over existing Marine SCR and switched communications assets. The number of processors and peripheral devices within a given node, and the network topology, will be dynamically reconfigurable.

3.2.9 PORTABILITY

The mobility and portability of the MLS-IAS will vary with echelon. Portability will be governed by the selected MCHS hardware. The system should be as lightweight and compact as technology permits. Each component of the system will be capable of being carried by two Marines. The intermediate IAS (MEUs, divisions, wings, FSSGs, groups, regiments) shall be team portable with no piece or equipment requiring more than two Marines to transport it for extended periods. The single workstation configuration (battalions, squadrons) will be a very portable system capable of being carried by a single Marine for extended periods.

3.2.10 SYSTEM SETUP

The MLS-IAS hardware shall meet system set-up requirements identical to those for the system high mode IAS. The time required for system initialization and verification of secure operation will be minimized.

When the equipment has been placed in a storage condition for a period of 365 days or less, it must be capable of being placed in an operational mode in less than three days.

3.3 DESIGN AND CONSTRUCTION

The MLS-IAS hardware design and construction will be consistent with those for the MCHS hardware. This includes:

- Materials
- Electromagnetic radiation
- Nameplates and product markings
- Workmanship
- Interchangeability
- Safety
- Human engineering
- Nuclear Control

3.3.9 SYSTEM SECURITY

The MLS-IAS shall support security in accordance with the requirements of DoD Regulation 5200.1-R, "Information Security Program Regulation," DoD Directive 5200.28, "Security Requirements for Automatic Data Processing," and DoD Manual 5200.28-M, "Security Manual -- Techniques and Procedures for Implementing Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems." For SCI information the protection requirements contained in DCID 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks" which is

implemented in DIAM 50-4, "Security of Compartmented Computer Operations" also apply.

Significant requirements imposed on ADP systems by these regulations and directives include:

Labelling. ADP systems designed to enforce a mandatory security policy must store and preserve the integrity of all applicable classification and sensitivity labels for all information. Labels exported from the ADP system must be accurate representations of the corresponding internal sensitivity labels and meet requirements for the marking of classified documents.

Within MAGIS, information will exist at various sensitivity levels. The MLS-IAS system can be expected to store and process information spanning this range of sensitivities. Within the established DoD classification scheme, there are five hierarchical sensitivity levels defined for classified data as shown below:

UNCLASSIFIED - information whose disclosure will not cause damage to the national interests.

SENSITIVE BUT UNCLASSIFIED - information which is not expected to damage the national interests, but which should not be widely distributed.

CONFIDENTIAL - information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security.

SECRET - information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

TOP SECRET - information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

DoD security regulations also provide for a formal "need-to-know" policy which utilizes non-hierarchical categories (or compartments) defined by the Special Access Program. Information at any of the hierarchical levels of sensitivity may be restricted by placing it in a compartment. Such information is generally referred to as Sensitive Compartmented Information (SCI). It is the combination of the hierarchical sensitivity label and compartment which defines a data object's overall sensitivity level.

There are additional restrictions which may be placed on information in the form of caveats. Although these serve a function similar to that of compartments, they are usually broader in scope. There are no specific clearances that correspond to the caveats; instead, specific properties of individuals (such as citizenship or authorship) are identified. The IAS will control data in accordance with all caveat control

information supplied by either the originator nation or data source. Some caveats in use include:

Restricted Data (RD)- Information concerning nuclear materials and weapons.
Formerly Restricted Data (FRD) - Information which was previously RD and is treated as RD for purposes of foreign dissemination.
Originator Controlled (ORCON) - Distribution controlled by the originator.
NATO - Information circulated within and by NATO.
Releasable to UK (RELUK) - Information which may be disseminated to properly cleared citizens of the UK.

Mandatory Security. ADP systems enforcing a mandatory security policy must include a set of rules for controlling access to information based directly on comparison of the individual's clearance or authorization for the information and the classification or sensitivity designation of the information being sought. The Mandatory Access Control (MAC) rules must accurately reflect the laws, regulations and general policies from which they are derived. We note that DoD regulations provide an ordering of information sensitivity in the form of a partially ordered lattice. This allows dominance relationships between a user's security clearance and a data object sensitivity level to be determined. Based on this relationship, the MAC can determine what access, if any, a particular user should be granted to a data object.

Discretionary Security. ADP system enforcing a discretionary security policy must include a set of rules (i.e., Discretionary Access Controls (DAC)) for controlling and limiting access to information to those individuals who have been determined to have a valid need-to-know. These rules are designed to limit access to those individuals who require access to the information in order to perform their official duties. These rules are discretionary in that the owner of a particular data object within the system determines what access rights to grant other individuals. These decisions are not based on formal interpretation of security regulations but upon operational need. These rules are applied only after determining that access to the information is allowed under the mandatory security policy.

Accountability. Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. To assure accountability, the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time, and without undue difficulty. This requires that an ADP system provide mechanisms for the positive authentication of all individuals accessing the system and that an audit log/file be maintained which reflects a history of system activity.

Assurance. Systems that are used to process or handle classified or other sensitive information must be designed to guarantee correct and accurate interpretation of the security policy and must not distort the intent of that policy. Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life-cycle.

Within these general requirements, evaluation of the MLS-IAS mission provides the basis for establishing a set of required secure automation capabilities. These are summarized in Table 3.3-1. The overall MLS-IAS mission can be aggregated into four broad functional categories as shown in the column headings. Electronic Information Exchange covers the exchange of digital data between the MLS-IAS and external systems via communications linkages. Data Fusion is the principle process within the MLS-IAS covering the analysis of data and generation of intelligence products. Liaison/Coordination covers those functions which allow the IEW staff to work effectively and cohesively. Finally, bulk data exchange supplements the interface to external systems when large volumes of data are required.

Table 3.3-1. Automation Security Requirements

	Electronic Info Exchange	Data Fusion	Staff Liaison/ Coordination	Bulk Data Exchange
Data Communications - MLS - IAS	 X X	 X	 X	
MLS File Management	X	X		X
MLS Database Management	X	X		X
Data Archive - Labelled - UN-labelled				 X X
Labelled Hardcopy Output		X	X	
Sensitivity Validation/ Assignment	X	X		X
Sanitization/Downgrading	X	X		

3.3.9.1 REQUIRED CLASS OF PROTECTION

The Trusted Computer Security Evaluation Criteria (DoD 5200.28-STD) defines seven classes of ADP systems. These span the range of information protection and system assurance achievable with existing technology. Class D systems provide no protection or assurance features adequate to meet one of the other classes. C-level system provide only DAC, and B1 through A1 class systems provide both MAC and DAC coupled with increasing strength of the underlying protection mechanisms and system assurance. This rating system is the only accepted standard for determining the strength of security mechanisms provided by Trusted components and for comparing the capabilities of competing components.

Establishing a target system class for the MLS-IAS, provides accepted guidance on the security features required to insure adequate protection of classified information within the MLS-IAS operating environment. At the same time, proper

determination of a target class limits the likelihood that the system will be over-designed. Over specification of such systems can significantly limit available COTS/NDI options, lead to increased development costs, and have a negative impact on system maintenance and operation.

We note that designing to the DoD 5200.28-STD criteria, provides reasonable assurance that the system will meet both operational requirements and DoD security regulations. This is not a sufficient condition for system acceptance however. The MLS-IAS must ultimately be accredited for use in a specific environment. The accreditation process is distinct from the certification process. System certification makes it far more likely that the system will be accredited, but it is not a pre-requisite nor a guarantee.

In establishing a target class for the MLS-IAS, the first step is to define the operational environment and the Trusted Computing Base (TCB). The TCB is defined as the totality of protection mechanisms within a computer system which is responsible for enforcing security. As discussed in Paragraph 3.2.1, the MLS-IAS must operate in garrison, shipboard, and on the battlefield. In each of these environments, we postulate that each node (i.e, MEF/MEB or Intermediate) will provide a distributed Trusted Computing Base (TCB) and each single workstation a standalone TCB. Access to each TCB will be restricted (using physical security) to insure that only personnel possessing a minimum of a Top Secret/Special Background Investigation (TS/SBI) clearance will have access to the system. These individuals need not be cleared for all SCI compartments supported on the TCB. This situation is shown schematically in Figure 3.3-1.

This definition of the TCB boundary, implies that interfaces between MLS-IAS nodes (distinct TCBs) and external systems will occur via a structured information import/export capability. Such an architecture can support multilevel information exchange between the TCBs along with interfaces to both SCI and GENSER external systems. The only significant limitation is that it precludes a user at one node from directly accessing processing/storage resources at another node. This does not appear to be a required capability of the objective system. The advantage of this approach is that the USMC digital communications backbone can be excluded from consideration in assessing the TCB.

CSC-STD-003-5 and CSC-STD-004-85 provide guidance for applying DoD 5200.28-STD to specific environments. This allows one to construct a system risk index and establish an appropriate target system class based on the type of application, expected user profile, and sensitivity of information to be protected. Table 3.3-2 summarizes the result of applying this methodology for "Open Security Environments". An open security environment is one in which either some developers are not cleared to sufficient level to allow presumption that they have not introduced malicious logic, or system configuration management is not adequate to

protect against the introduction of malicious logic. This case must be assumed due to the use of COTS software within the system.

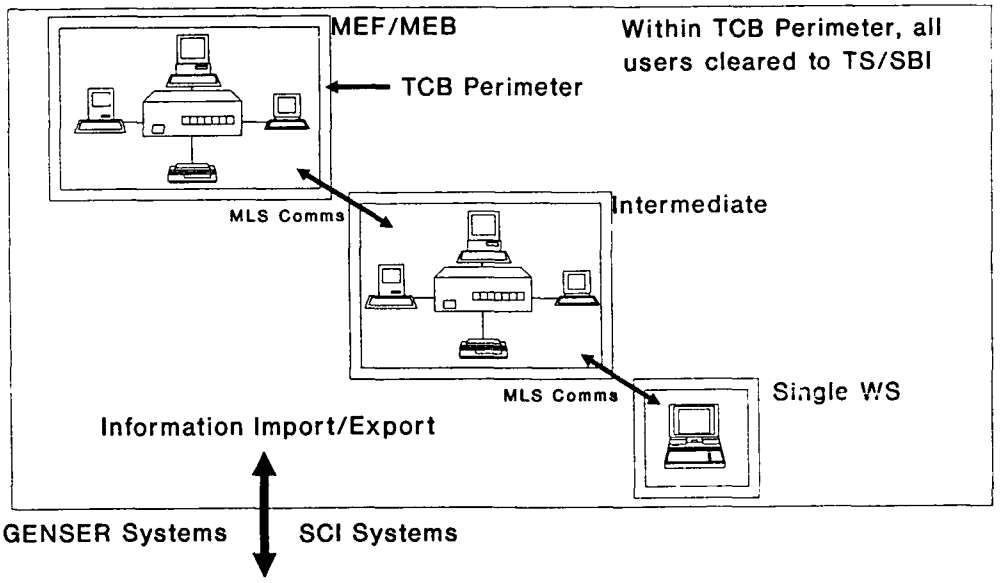

Figure 3.3-1. MLS-IAS TCB Boundary

Table 3.3-2. Minimum System Evaluation Class for Open Security Environments

Minimum Clearance or Authorization of System Users	Maximum Classification/Sensitivity of Information in the System						
	U	N	C	S	TS	1C	MC
U	C1	B1	B2	B3	•	•	•
N	C1	C2	B2	B2	A1	•	•
C	C1	C2	C2	B1	B3	A1	•
S	C1	C2	C2	C2	B2	B3	A1
TS(BI)	C1	C2	C2	C2	C2	B2	B3
TS(SBI)	C1	C2	C2	C2	C2	B1	B2
1C	C1	C2	C2	C2	C2	C2[1]	B1[2]
MC	C1	C2	C2	C2	C2	C2[1]	C2[1]

Note: Environments for which either C1 or C2 is given are for systems that operate in system high mode. No minimum level of Trust is prescribed for systems that operate in dedicated mode. Categories are ignored in the matrix, except for their inclusion at the TS level. "N" refers to sensitive but unclassified data.

[1]It is assumed that all users are authorized access to all categories present in the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

[2]Where there are more than two categories, at least a class B2 system is required.

As indicated by the highlighted region in Table 3.3-2, it is postulated that the appropriate target rating for the MLS-IAS TCB is B2. This is predicated upon the assumption that all users are cleared to at least an TS/SBI level and that the system will store and process data spanning the full range of hierarchical classification levels plus multiple compartments. A class B1 system would be adequate if all users were cleared for at least one compartment of data in the system and the system were restricted to a maximum of two compartments of data. Alternatively, as the minimum clearance level of users of the MLS-IAS is reduced, a B3 or A1 system would be required. Note that the limits of existing technology (class A1 systems) are not deemed adequate to protect multiple compartments of data if users with less than a Secret clearance are granted access to the system.

The U.S. Army CASS definition, which is being utilized as the basis for the MCASS, also identifies B2 as the target class for all systems which store, process, or transmit sensitive data. This provides a further basis for use of this class as the target in our design. In particular, the following requirements, by CASS reference number, have been defined:

- CASSASCA030 - The COTS software layer shall demonstrate compliance with a B2 security level as defined in DoD-5200.28 STD.
- CASSASCA045 - COTS software layer shall demonstrate compliance with a B2 security level to process multiple levels of classified data in a manner that provides data integrity and security protection as defined in DoD-5200.28 STD.
- CASSASCA050 - COTS software layer shall demonstrate compliance with a B2 security level to store multiple level of classified data in a manner that provides data integrity and security protection as defined in DoD-5200.28 STD.
- CASSASCA051- Shall shall demonstrate compliance with a B2 security level to receive multiple levels of classified data in a manner that provides data integrity and security protection as defined in DoD-5200.28 STD.

The above guidance applies to the TCB as an entity. Hence, for a distributed system as envisioned for the MLS-IAS, one must consider all of the system components operating in concert. In consequence, it is not necessarily sufficient to simply utilize B2 Trusted components. The interactions of these components must also be considered. An example is shown in Figure 3.3-2. This demonstrates a "Cascade Condition". In this case, the clearance level of the users on each processor and the sensitivity level of the information processed are commensurate with a B2 class system. By networking the system together however, we have a created a path by which a Confidential cleared user can access Top Secret data by defeating a B2 class mechanisms. This condition can be alleviated by upgrading one of the processors to a class B3 system. In the proposed MLS-IAS system, a similar condition will not exist since the user clearance levels and supported information sensitivities will be uniform across system elements. However, other more subtle problems may arise.

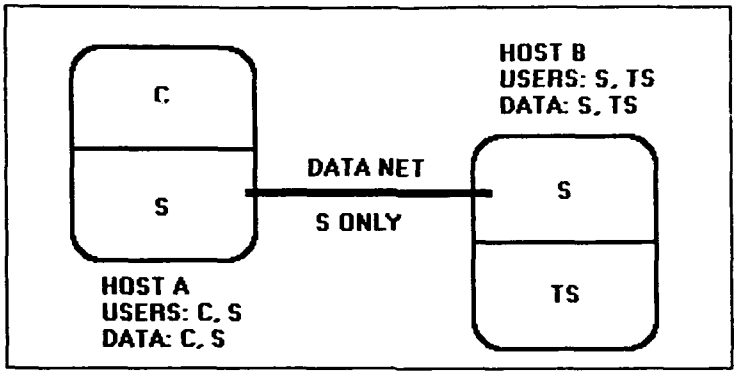

Figure 3.3-2. Cascade Condition

3.3.9.2 SYSTEM SECURITY POLICY

The MLS-IAS will enforce a system wide security policy which reflects DoD security regulations and directives including those relevant to the Special Access Program. Consistent with the requirements of DoD 5200.28-STD, a security policy model for the system must interpret the DoD policy in terms of entities internal to the MLS-IAS automation system. Based on existing systems, there are a number of viable approaches to specification of the system security policy model. These include access control policies, such as the Bell and La Padula model, and non-interference models as used by SunOS/MLS and LOCK programs. There is no preference for any particular approach to specifying the system security policy so long as it meets all requirements for system certification.

It is anticipated that the MLS-IAS will be developed from a set of Trusted components. In such a partitioned TCB, the system security policy model may be composed of multiple policy models which interpret the DoD policy for specific subsystems within the MLS-IAS. In this case, it must be possible to aggregate the models into a cohesive whole which clearly delineates:

- the mapping between entities within each model
- the domain in which each model is applicable
- conditions under which information can securely cross domain boundaries.

In the remainder of this section, minimal requirements for the security policy model elements which address operating system, database management, and data network elements are identified. Extensions to these basic elements, which interpret DoD policy to meet specific requirements of the MLS-IAS system, are then addressed. A formal policy model for this extended functionality must be developed as part of the system design process. This should be done following selection of the COTS Trusted components to insure a complete and consistent system model.

Security policy models deal with abstract entities and the rules covering the interaction between these entities which insure that information is not compromised. To aid in the discussion which follows, it is helpful to define the notion of "Subjects" and "Objects".

OBJECTS - Objects represent the passive, data carrying entities within the system and may include records, blocks, segments, files, directories, data dictionaries, data tables, messages, programs, and I/O devices. Associated with each object is a vector which describes its sensitivity level, discretionary access restrictions, and other security relevant information.

SUBJECTS - Subjects represent active entities within the system which cause information to flow between objects or alters the system state. These include users, processes acting on behalf of a user, and internal software processes which provide services to other subjects. Associated with each subject is a vector which describes its clearance level, the user on whose behalf it is operating, and other security relevant information.

3.3.9.2.1 Operating System Policy

As a minimum, it is expected that the OS policy model will provide an interpretation of DoD policy in terms of the interaction between users and aggregates of data maintained by the system. Objects can be viewed as containers of data and should include:

- Memory Blocks
- Buffers
- Queues
- Files
- Devices

The policy model must support the concept of sensitivity labels, which have a hierarchical and non-hierarchical component, and Access Control Lists (ACLs) which define discretionary access permission on a named individual basis. Both labels and ACLs must be associated with every object. The model must also support the concept of single and multilevel devices. For multilevel devices, a minimum and maximum sensitivity level supported by the device should be supported.

Subjects will include all active entities in the system, such as the users and programs, which cause information to flow between objects. Note that certain devices, such as disk controllers, may also be considered as subjects. For subjects external to the TCB, there must be an associated clearance level and a named individual on whose behalf the subject is operating.

The policy model must define those conditions under which access by subjects to objects is allowed. This must include distinction between read, write, and no access as a minimum. Access must be restricted in accordance with DoD regulations. As a minimum, this must include mandatory (MAC) checks based on the relationship of the subject clearance level and the object sensitivity level. Read access is allowed only if the subject's level dominates the object's level. Dominance requires that the hierarchical component of the subject's level be greater than the hierarchical component of the object's level and that the non-hierarchical component (compartments and caveats) of the subject include all compartments and caveats associated with the object. Write access is allowed only if the level of the object dominates that of the subject, and read/write access requires they be equivalent. Access may be further restricted by the access permissions defined for the individual by the object's ACL.

3.3.9.2.2 Database Policy

The RDBMS security policy must interpret DoD policy in terms of the unique organization of data and fine grained data storage inherent in a database. Data objects recognized by the RDBMS policy should include:

- Databases
- Relations (tables)
- Tuples (rows)
- Fields (data elements)
- SQL data definition and data manipulation requests
- Responses

The RDBMS policy should recognize the concept of a subject (user) external to the DBMS and internal subjects responsible for creating, modifying, deleting, and querying the database. The policy should incorporate the concepts of sensitivity labels, ACLs, users, etc. in a manner consistent with the OS policy. The concepts of MAC and DAC should be defined such that all transactions between subjects external to the RDBMS and the RDBMS occur in a manner that is consistent with DoD regulations.

The RDBMS policy should explicitly deal with the interface between the RDBMS and subjects/objects under the OS policy external to the RDBMS. This must provide a definition of how data is imported to the RDBMS and how it is interpreted to insure that data is created, modified, and deleted securely. It is also desirable that the conditions under which data integrity and consistency is assured be identified.

For queries, the policy should indicate how the RDBMS insures that all data to which the querying subject is authorized (MAC and DAC) is included in the generated response. It should indicate how the data is returned to the querying subject and how its sensitivity level is derived. In general, this will reflect the maximum sensitivity of

information used in generating the response. However, policies dealing with aggregates of data and potential inferences may be incorporated which would modify the sensitivity of returned data.

3.3.9.2.3 Network Access

The network policy must interpret DoD policy in terms of natural data communications entities such as datagrams, message headers, message bodies, peer entities, connections, data switches, etc. It should associate sensitivity labels, ACLs, and user identification with these entities in a manner consistent with that for the OS policy.

The network policy should deal explicitly with the interface between the network and the subject/objects external to it. This should identify how subjects make network requests, how data is provided to the network and mechanisms for insuring its labelling consistent with the OS concept of sensitivity, and how MAC and DAC are enforced to insure that data flows securely over the network.

It is expected that the network policy will support the exchange of arbitrary data over the network. The flow of this information should be restricted such that:

- Subjects can only access data whose sensitivity label is dominated by the subjects clearance level
- Subjects can only access data in a manner consistent with the restrictions imposed by ACLs associated with the source objects.

3.3.9.2.4 Imported Data

It is recognized that the majority of data imported into the TCB will be provided by external systems which can not be relied upon to provide machine readable data labelling. In such cases, the data must be imported via a single level device and the TCB shall label the data with the device sensitivity level. Such labels are subject to review and validation by authorized users of the MLS-IAS, but any alteration of the sensitivity level associated with the data is based on human action outside of the TCB security policy. However, if the imported data was exported in a multilevel format by another TCB (either another MLS-IAS node or some other system) then the MLS-IAS TCB should correctly interpret the sensitivity labels and place the data in appropriate objects. Such data must be imported using a multilevel device.

Policy. The MLS-IAS will explicitly recognize the existence of labelled, formatted data external to the TCB. For each external format supported by the system, the TCB will provide the ability to transform such data on input into a collection of internal storage objects which accurately reflect the sensitivities indicated by the external labels. An authorized user must identify the labelling/format convention used for the source data and verify the data source prior to importing such data.

Risks. Given improperly formatted or labelled data, there is a risk that the TCB will assign an inappropriate sensitivity level. This risk is limited provided that human source validation is required and that the TCB refuses to import data upon detection of an unrecognized label or improper data format.

3.3.9.2.5 Message Log/Journal Operations

It is required that the MLS-IAS perform logging and journaling of all incoming and outgoing message traffic. These logs/journals must reflect all message traffic and will generally include only information associated with a message which is at a low sensitivity level to insure they can be readily reviewed and maintained. However, the overall classification of the source messages may span the full range of sensitivities supported by the system. Hence, in preparing message logs and journals, information from the source messages must be extracted and sanitized. This is facilitated by the fact that military message traffic is rigorously formatted in accordance with established standards and specific fields will contain information which has a fixed, low sensitivity, level for all messages. This includes such information as the destination(s), DTG, message type, and source. The MLS-IAS should be able to automatically parse formatted military messages, extract required identifying information of a level compatible with the desired sensitivity of the log/journal, and create a prototype entry. This should minimize any need for manual transcription/sanitization of data in the source message. Such entries could be subsequently reviewed and edited by authorized individuals responsible for log/journal maintenance.

Policy. The MLS-IAS will explicitly recognize the multilevel nature of formatted military messages. This should include MTS and USMTF message formats as a minimum. It will be possible for the TCB to extract specific fields from a message and assign this information to an object with a sensitivity level established by the SysAdmin. The specific fields to be extracted will be defined for each message format and type supported by the system. In performing this transformation, the TCB will verify that the message is properly formatted in accordance with the appropriate standards and that each extracted field is properly formatted and contains only legal data values. The notions of properly formatted and legal data values must be defined for each message format and message type. Once the appropriate data has been sanitized, the actual creation of the log/journal entries can be performed in accordance with the OS and RDBMS policies.

It is noted that formal security policies have been developed which treat military messages as true multilevel objects, notably the Military Message System policy developed at USN/NRL. However, these have proven intractable as part of general purpose systems. The policy proposed for the MLS-IAS is significantly more restrictive and should pose no significant implementation problems.

Risk. There is a risk of information compromise if the TCB attempts to extract information from an improperly formatted message or one in which highly sensitive data has been placed in an improper field. The former risk can be mitigated by requiring the TCB validate the message format. In particular, fields such as sources, destinations, message types, DTGs, etc. can all be validated against known values. The latter risk is limited since both the source messages and logs/journals will be reviewed by system users and the logs/journals are not directly accessible except to authorized users of the system.

There is also a potential for covert signalling exploitable by observing the order in which log/journal entries appear. However, this would have a very low bandwidth during any normal operation.

3.3.9.2.6 User Alerting

It is a natural expectation within a tactical intelligence system that users will be notified promptly of messages/mail requiring their attention. Such alerting should be provided independently of the sensitivity level associated with the message/mail and the current clearance level associated with the active user session. To provide such alerting, and allow the user to efficiently review a list of arriving messages, it is desirable that a log of incoming messages/mail be maintained at the minimum level authorized for the user (insuring it can be read by any user Subject) and that an alert be posted to the user's display terminal if logged on.

Policy. For formatted military messages, the policy extension proposed for allowing automated log/journal entries is sufficient. The sanitized information extracted from each message can be placed in an object at the user's minimum clearance level and utilized to create a user log entry for each addressee. For internal electronic mail messages a similar approach will be used. The TCB shall recognize the electronic mail is inherently multilevel. It will be possible to extract the source, destination, and DTG fields as a minimum and place these in an object at each addressees minimum clearance level. It is relatively simple to verify that these fields contain known values. If a mail message's subject is allowed to be an arbitrary text string, it may not be practical to automatically validate the true sensitivity of this information. Creation of the log and writing of an alert message can proceed under the normal OS/RDBMS policy.

Risks. These are similar to those discussed for the message log/journal operations, and it should be possible to constrain them to an acceptable level.

3.3.9.2.7 Sensitivity Validation

The MLS-IAS must support the validation of information sensitivity. This includes the potential need to upgrade the sensitivity of data aggregates as well the need to downgrade information extracted from highly sensitive source documents. With the exception of rigorously formatted data, such as the military messages discussed above, automated sensitivity validation is beyond the state of the art. As such, the MLS-IAS TCB will not support an explicit policy regarding the sensitivity of data aggregates or subsets. All such sensitivity adjustments must be performed by an authorized individual. The TCB will accept such adjustments provided that the user has been properly identified, his authorization authenticated, and actions are invoked via a Trusted Path.

3.3.9.2.8 DATA INTEGRITY

It is not required that the MLS-IAS support a formal data integrity policy. However, if an integrity policy is specified for a Trusted component, it must be enforced. As a minimum, the system must provide data integrity and consistency mechanisms in accordance with modern software engineering practices. Such mechanisms are, however, external to the TCB.

3.3.9.3 SECURITY SERVICES

In this section, we delineate specific security services which the MLS-IAS will provide to enforce the system security policy, provide assurance that the mechanisms are invoked, and provide for establishing system parameters. As a minimum, these mechanisms must include the requirements defined in DoD 5200.28-STD for class B2 systems. These requirements are summarized in Table 3.3-3. The mechanisms may be distributed over multiple TCB partitions so long as the system as a whole meets all of the certification requirements.

Table 3.3-3. Summary of B2 System Requirements

1. All information must be labelled to accurately reflect its sensitivity
2. All users must be identified and their clearance level authenticated
3. MAC must be enforced based on a user's clearance and the sensitivity of data reflected by its associated label
4. DAC must be enforced based on a user's identification and permissions established by the owner of a data object
5. All data exported from the system must be labelled with human readable labels which accurately reflect its sensitivity

6. The TCB must be unbypassible and tamperproof. This can be demonstrated using a combination of architectural features, audit mechanisms, and tests.

7. A Trusted Path providing assured direct communication between a user and the TCB must be utilized during security critical operations.

3.3.9.3.1 Sensitivity Labels

The system will support sensitivity labels which are capable of representing all standard DoD and NATO classification markings (hierarchical level and compartments) and caveats (CASSASCA150). As a minimum, the system will provide the ability to handle up to five hierarchical sensitivity levels and up to 32 non-hierarchical elements (compartments and caveats) at a given time.

3.3.9.3.2 Information Labelling

The MLS-IAS shall maintain labels for all data objects within the system which unambiguously reflect the sensitivity of the data contained in the object. This includes all memory objects which are allocated to a user process, files, databases, message, queues, buffers, etc.

3.3.9.3.3 Device Labels

The MLS-IAS shall support both single and multilevel hardware devices as defined in DoD 5200.28-STD. For single level devices, an information sensitivity level, from within the range of sensitivities supported by the system, will be assigned to the device. This sensitivity label will be utilized to enforce MAC between user subjects and the device. Alteration of the sensitivity label for a single level device will be possible by the SysAdmin when the device is inactive (see 3.3.9.3.12).

For multilevel devices, a range of information sensitivities for the device, bounded by the sensitivity range supported by the systems, will be established. It will be possible for user subjects to access the device provided their clearance level is within the specified range.

All devices will support an ACL to allow restricted device access on a named individual basis.

3.3.9.3.4 Subject Labels

Each subject will have associated with it a label which unambiguously defines the sensitivity level at which it is operating. The TCB shall immediately notify a terminal user of any change in the security level associated with that user during an interactive

session. It shall be possible for a user to query the TCB for the full sensitivity level associated with any subject running on behalf of the user.

The system will also establish the individual user on whose behalf each subject external to the TCB is operating. This information will be used for enforcement of the DAC policy.

3.3.9.3.5 Labelling Imported Information

DoD 5200.28-STD provides no specific guidance on mechanisms for establishing the appropriate sensitivity level of imported information. Information entering the MLS-IAS may come either from a single or multilevel device. For single level devices, all imported information will be placed in a storage object which reflects the current sensitivity level associated with the import device. This sensitivity level will be provisional and subject to review and adjustment by an authorized individual or in accordance with the security policy for specific formatted data.

Information imported from multilevel devices must have embedded sensitivity labels which unambiguously identify the sensitivity level of the data, are comprehensible by the TCB, and are within the minimum and maximum range of sensitivities specified for the device. Failure to meet these conditions will be an auditable event and should cause immediate deactivation of the import device. The TCB shall be capable to logically separating properly labelled multilevel data, converting between the input label format and that used internally by the TCB, and placing the data in storage objects with appropriate sensitivity labels. This is consistent with CASSASCA178, which requires the system to read the security level of incoming messages.

3.3.9.3.6 Labelling Exported INFORMATION

Information exported to multilevel devices is required to be labelled in accordance with DoD regulations. It is not necessary to label information exported to single level devices. All information exported to a single level device is implicitly labelled with the sensitivity level associated with the device. The MLS-IAS will support four types of multilevel devices: display; hardcopy output; archive magnetic media; and data communications.

Video Displays. Video display screens represent the primary media for interaction with users of the MLS-IAS system. The display screen shall be a multilevel device within the system with the minimum and maximum information levels supported determined by the clearance level of the currently active user. These levels will be established as a part of the user logon process. The video display will support the concept of virtual displays in which each virtual display may contain information at a different sensitivity level. Each virtual display will be associated with a unique subject running on behalf of the user. The preferred approach will be to present the virtual display as a collection of windows on the physical display screen. The

alternative will be to allow the user to switch between virtual displays, with only one displayed at a given time.

Each virtual display screen will include a human readable sensitivity label which reflects the maximum sensitivity level of information which may be displayed (CASSASCA200,CASSASC210). A floating information label which reflects the sources of data used in building the data set being displayed, such as defined for the DIA CMW program, may also be provided as an aid to the user. A human readable sensitivity label will also be provided on the display which reflects the sensitivity of the subject which will currently receive user input. A positive indication will be provided on the display any time the user's input level is changed.

Hardcopy Output. The MLS-IAS will support printer and plotter hardcopy output devices. A minimum and maximum sensitivity level supported by each hardcopy output device will be settable by the SysAdmin. Altering these levels will be possible only when the device is inactive. All output will be labelled at the top and bottom of each physical page to indicate the highest sensitivity level of information contained in the data (CASSAMID020).

Archive Media. The MLS-IAS will support both tape and disk multilevel archive media. The minimum and maximum sensitivity level supported by the archive device will be settable by the SysAdmin. Altering the sensitivity level will be possible only when the device is inactive. All data on the archive device must have an associated sensitivity label which unambiguously identifies its sensitivity. The sensitivity labels may be either in an internal format or a human readable format. The format for recording both the data and the sensitivity labels must be specified in the system documentation.

Data Communications. The MLS-IAS will support multilevel data communications ports. A minimum and maximum sensitivity level supported by the device will be settable by the SysAdmin. Altering the sensitivity level will be possible only when the device is inactive. All data packets transmitted over a multilevel channel must have a sensitivity label which unambiguously reflects the sensitivity level of the data bound to the data. This label may either be an internal representation or a human readable label depending on the destination of the data. Internal to the MLS-IAS, it is desired that the sensitivity level of each data packet be identified using the label field of the IP protocol header in accordance with the RIPSO (Revised IP Security Option) specification.

3.3.9.3.7 Identification And Authentication

The TCB shall identify and authenticate each user of the MLS-IAS TCB prior to initiating any other action that the TCB is expected to mediate. As a minimum, identification will be based on comparison between the user's identifying name (ID) and password with those stored in the TCB's user database (CASSASCA230). This

exchange of information between the TCB and user must be supported by a Trusted Path initiated by the user. In general, user authentication will occur when the user first logs-on the system. However, certain actions, such as attempts to initiate a new session at a different classification level, will require re-authentication of the user.

Following user authentication, the TCB shall insure that any subjects (processes) created to act on behalf of the user run at a classification level which is dominated by the user's clearance level. The user's ID will be used as the basis for enforcing DAC.

It is desirable that the MLS-IAS provide a distributed authentication service in which the user need only identify himself to a single TCB entity for each active session. The various TCB partitions should securely and transparently exchange identification and authentication information required to enforce the system security policy.

3.3.9.3.8 Discretionary Access Controls

The MLS-IAS shall enforce DAC in accordance with the requirements of DoD policy (CASSASCA240). The system will enforce the basic concepts of read, write, and no access as a minimum. All DAC controls will be based on ACLs associated with each data object and a named individual. ACLs may define permissions in terms of aggregates of individuals to simplify specification and maintenance. Within the MLS-IAS, such groups could define user functional responsibilities. The SysAdmin will be provided mechanisms to establish and modify groups as part of the user database. It shall be possible to restrict read and write access to an ACL to the owner of the associated object. A consistent method of specifying ACLs and determining access permissions must be used within all of the TCB partitions. The access concepts supported by each partition may be different. For example, the RDBMS partition could support distinct delete and update access modes rather than write access.

The OS partition of the TCB will be responsible for enforcement of DAC on files, memory, I/O ports and other system hardware resources. The OS will restrict subject access to the following based on owner designated ACLs:

- File system directories and files
- Peripheral devices
- Supported IPC channels (pipes, sockets, shared memory, etc.)

The RDBMS partition of the TCB will be responsible for enforcement of DAC for the databases, to include data tables, data definition databases, data dictionaries, and stored procedures.

The network partition of the TCB will be responsible for enforcement of DAC for data communications channels between hosts within an MLS-IAS node and to external systems.

3.3.9.3.9 Mandatory Access Control

The MLS-IAS shall enforce MAC in accordance with the requirements of DoD policy (CASSASCA250). The system will enforce the basic concepts of read, write, and no access as a minimum. Finer grain access rights are desirable and may vary within each TCB partition so long as no exploitable channels result. MAC decisions will be made in accordance with DoD security policy based on the clearance level associated with a subject acting on behalf of the user and the sensitivity level associated with the data object. MAC will be enforced uniformly for all data accesses performed by subjects external to the TCB.

The OS partition of the TCB will be responsible for enforcement of MAC on files, memory, I/O ports and other system hardware resources.

The RDBMS partition of the TCB will be responsible for enforcement of MAC for the system database to include data tables, data definition databases, data dictionaries and stored procedures.

The network partition of the TCB will be responsible for enforcement of MAC for data communications channels between hosts within an MLS-IAS node and to external systems. Between MLS-IAS entities, MAC enforcement will be based on the sensitivity of the transmitted data and the clearance level of the subject which is to receive the data. If the clearance level of the receiving subject must dominate the level of the data or the connection will be disallowed. Note that two-way communications can only be established between cooperating subjects operating at an identical sensitivity level.

3.3.9.3.10 Object Reuse

The system will insure that all information is purged from a storage object prior to its initial allocation to a subject from the TCB's pool of unused storage objects.

3.3.9.3.11 Message Handling

The system will be capable of recognizing the inherent multilevel nature of formatted military messages as defined by the system security policy. Mechanisms will be provided which can verify and extract low sensitivity header information from such messages in an automated fashion. It will be possible for the SysAdmin to enforce a manual review of such information prior to its being downgraded and released for general access within the system.

3.3.9.3.12 System Administration

Administration of the MLS-IAS system shall be vested in a identifiable individual(s) (System Administrator). It shall be possible to logically separate the administrative functions required to support host Trusted OS, RDBMS, and LAN. These functions will involve administration of security critical elements of the system, and hence their exercise must be carefully controlled and limited to highly trusted individuals to insure secure operation of the system.

The system administration utilities will support the following services:

USER DATABASE - A database of users authorized access to the MLS-IAS will be maintained by the system. This database will contain sufficient information to identify each individual user, a name by which the user is known to the system, the range of classification which the user is authorized based on his/her clearance, any additional access privileges, and password or other information required for positive identification of the user. This database will be protected from unauthorized access or modification by the TCB (see CASSASCA260).

AUDITING - The SysAdmin will be provided tools for controlling the collection of audit information (see 3.3.9.3.13), archiving audit data, and for the reduction and analysis of audit data. It will be possible for the SysAdmin to specify subsets of security critical events to be audited and to control auditing on a per-user basis. The audit parameters established by the SysAdmin will be protected from unauthorized access or modification.

ARCHIVE/RECOVERY - The system will provide tools for archiving and restoring specified subsets of the MLS-IAS file system and databases. Both data and executable programs may be archived/restored. It is desired that archives be written in a multilevel format consistent with the POSIX portable archive format (pax). Sensitivity labels which accurately reflect the sensitivity of all information in the archive must be unambiguously bound to the data.

FILE SYSTEM MANAGEMENT - Facilities will be provided which allow the SysAdmin to create, establish privilege levels, mount, unmount, and destroy a file system. It will be possible for the SysAdmin to specify minimum and maximum sensitivity levels for a file system at creation time and to control access on a individual user basis through specification of an ACL for the file system. Tools will be provided to allow the SysAdmin to perform consistency and integrity checks on any file system and to modify the file system to restore it to a consistent state.

KEY MANAGEMENT - If the system supports embedded COMSEC functionality, utilities will be provided to allow the SysAdmin to load and unload cryptographic key variables.

SENSITIVITY LEVEL DATABASE - The system will maintain a database of sensitivity levels supported by the system. This will include all hierarchical classifications, SCI categories, and caveats. The database will provide a mapping between internal label representations and human readable sensitivity labels. This database will be protected from unauthorized access or modification by the TCB.

SYSTEM SET-UP - Tools will be provided to allow the SysAdmin to set-up and initialize the system in a secure state. System validation utilities will be provided to allow the SysAdmin to periodically establish the correct operation of TCB hardware or firmware mechanisms.

I/O DEVICE MANAGEMENT - Tools will be provided to allow the SysAdmin to specify the sensitivity level associated with each single level device and to establish a minimum and maximum sensitivity level for each multilevel device. It will also be possible to limit I/O device access on an individual user basis through the use of ACLs. Alteration of the security parameters associated with a given device will only be possible when that device is deactivated. It will be possible for the SysAdmin to deactivate a device and clear all associated storage buffers.

SYSTEM PURGE - It will be possible for the SysAdmin to selectively purge (also referred to as "sanitization") main memory, random access mass storage devices, and system queues and buffers (e.g., print queues, message queues, and display buffers) in accordance with the requirements of DIAM 50-4 and the Marine Tactical Automated Systems Security Guide (TBP)(CASSASCA070). Specific capabilities will include:

- The capability for the SysAdmin to selectively purge individual mass storage entities (CASSASCA080).
- The capability to initiate the purge of selected buffers in the communications hardware (CASSASCA090).
- The capability to initiate the purging of magnetic media (CASSASCA095).
- The capability to purge MCHS magnetic media within five minutes in accordance with DIAM 50-4 (CASSAPER020).
- The capability to continue to perform normal database access request during sanitization exclusive of the specific table being sanitized (CASSASCA100).
- A completion status parameter to the calling application program at the end of the requested sanitization process (CASSASCA120).

ALTER SENSITIVITY LABEL - It will be possible for the SysAdmin to change the sensitivity label associated with any file or database storage object in the system. Alteration of the sensitivity label associated with any storage object may only occur when the object is inaccessible to user subjects (applications programs). A means of insuring that the object is not being accessed by a user subject will be provided.

DATABASE ADMINISTRATION - It will be possible to establish a distinct DBMS Administration role in the system. This could be the SysAdmin, but need not be. The following functions will be supported and restricted to the DB Administrator or individuals authorized by the DB Administrator:

- Archive of databases and tables
- Restoration of databases and tables
- Modification of a database structure definition
- Definition of database ACLs
- Establishment of sensitivity level restrictions for a database
- Sanitization of database storage objects
- Bulk loading of database data

NETWORK MANAGEMENT - The system will maintain network management tables which determine available LAN data communications resources and restrict communications channels in accordance with MAC and DAC. It will be possible to restrict access to these functions to a distinct LAN Administrator if desired. This could be the SysAdmin. The Administrator will be able to edit these tables to allow for alteration of:

- Network configuration and host addresses
- Minimum and maximum sensitivity range for communications with each host
- ACLs specifying allowable data paths in accordance with DAC. It is desirable that this provide control on a named individual level, but shall provide control on a host-to-host basis as a minimum.
- LAN activations/de-activation
- Sanitization of network storage objects

The TCB will protect these tables from unauthorized access and modification.

Network diagnostic tools will also be provided to allow the Administrator to query the status of each host and to monitor network traffic to determine anomalous behavior which could impact on proper network

operation. Access to these tools will be limited to the Administrator and must operate via a Trusted Path.

The system administrative tools should provide a uniform, menu driven interface for all functions. Access to these functions will be limited to the individual(s) designated as system Administrator(s). All security critical operations will require a Trusted Path between the Administrator(s) and the TCB. It is desirable that the Administrator(s) be able to access system wide administrative functions from a single host within a MLS-IAS node. This requires the capability to invoke a Trusted Path between hosts and which is not a requirement.

3.3.9.3.13 Audit

The MLS-IAS shall monitor, at the discretion of the SysAdmin, all security relevant events outlined in DoD 5200.28-STD to include (see CASSASCA000):

- Abnormal process terminations
- Attempts to violate control limits
- Invalid classification and sensitivity labels
- Log on/log off events and errors
- Attempts to execute data
- Attempts to change passwords
- Attempts to change DAC parameters (e.g., unauthorized ACL modification)
- Attempts to downgrade a file's or other data object's classification
- Any unique MTACCS C4I system defined relevant events
- Attempts to pass messages/data of a higher security classification than authorized level of the workstation or communications link.
- Attempts to create or copy data bases

Audit data shall allow the tracing of actions which affect security, or represents attempts to circumvent security, to an identified individual user. Immediate notification of the SysAdmin on the occurrence of a designated class(s) of security relevant events shall be selectable (CASSASCA020).

System audit information shall be written to a distinguished audit log, in accordance with the requirements of NCSC-TG-001, which is protected from tampering or access by individuals except as designated by the SysAdmin (CASSASCA010). It is desired that the audit log be maintained in a consistent format and on a single media type by each of the partitions which comprise the system TCB. (There are no standards for the formatting of TCB audit records at the present time). In the event that secondary storage allocated for audit data is exhausted, the system may either continue to run or initiate a controlled shut-down as selected by the SysAdmin. A warning message will be sent to the SysAdmin prior to the available audit media storage space becoming filled. If the SysAdmin is not logged onto the system at the

time of this event, the warning will be delivered as soon as the SysAdmin logs in. It will be possible for the SysAdmin to archive all audit data on removable storage media and to aggregate audit information from the various TCB partitions. Tools will be provided for the review and analysis of audit records. It is desirable that a single tool be provided which can be utilized for analysis of all audit data.

3.3.9.3.14 Architectural Features

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering consistent with B2 requirements. It will provide:

- Process isolation through provision of distinct address spaces under its control
- Internal TCB structuring into largely independent modules
- Logically distinct storage objects with separate access attributes (e.g., read, write)
- Separation of protection critical elements

3.3.9.3.15 Denial Of Service

The MLS-IAS shall provide controls and administrative tools to assist in the isolation, tracking, and safeguarding of the system against denial of service attacks (CASSASCA330). Within a given processing element, it will be possible to identify a subject, and an associated individual, making unusual or excessive demands on system resources. It will also be possible to identify devices which are imposing excessive I/O demands due to external actions. Network management tools will assist the SysAdmin in identifying the source of suspicious external events. It will be possible for the SysAdmin to selectively terminate a subject, force an immediate user log-off, or deactivate a device to limit system degradation.

3.3.9.3.16 Additional Network Services

It is desired that the network component of the MLS-IAS support functionality in addition to basic MAC, DAC, Identification, and Auditing services as discussed above. These services are valuable in addressing several classes of denial of service attacks and concerns over message integrity. These include:

- Message Stream Modification Protection to protect data and header fields from unauthorized/unintended modification. This can be provided by a variety of mechanisms including CRCs, message encryption, etc.

- Communications Authentication Integrity to insure that the communication is intended for the addressed peer entity and that source is the one claimed.

- Non-repudiation services to insure that unforgeable proof of shipment and/or receipt of data can be established.

3.3.9.4 PHYSICAL SECURITY REQUIREMENTS

The provision of COMPUSEC addresses concerns over the compromise of information to users or external automation systems. COMPUSEC does not address the potential threats due to physical attack or covert analysis of electromagnetic radiation (TEMPEST). A suitable physical protection boundary will be established about each of the MLS-IAS TCBs as shown in Figure 3.3-3. The physical boundary will be established in consideration of the local environment, distribution of equipment, and exclusion zone requirements as may be necessary to meet TEMPEST.

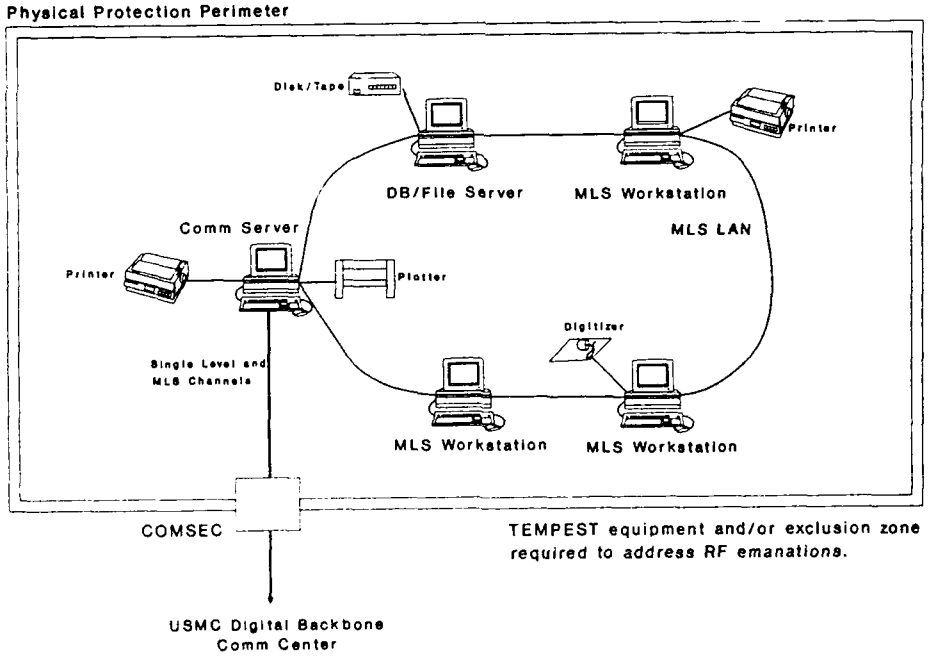

Figure 3.3-3. Physical Protection and COMSEC Perimeters

Physical protection of the MLS-IAS is required to protect against theft of system resources (particularly storage media), unauthorized access to human readable output, unauthorized access to user terminals, and protection of system hardware

from modification. It must also protect against the placement of passive "taps" which would allow signals generated by the system to be analyzed at a remote location. TEMPEST protection is aimed preventing the passive detection and analysis of signals generated by the processing elements, display hardware, and communications subsystem.

3.3.10 GOVERNMENT FURNISHED PROPERTY USAGE.

Not applicable.

3.3.11 COMPUTER RESOURCE RESERVE CAPACITY

The MLS-IAS shall be capable of expansion in regard to its responsibilities and functions. Both the hardware and applications software shall be upgradeable. Specific conditions under which such upgrades may be performed without requiring re-certification/accreditation of the system security features will be addressed in subsequent design documentation.

3.4 DOCUMENTATION

All documentation will be prepared in accordance with the requirements applicable MIL-STDs and DoD 5200.28-STD.

3.4.1 SPECIFICATIONS

Design specification for the systems will be prepared in accordance with MIL-STD-490 and applicable DiDs. All specification requirements of 5200.28-STD for B2 class systems will be met using a combination of COTS Trusted software documentation and supplemental material covering MLS-IAS specific extensions. This will include preparation of:

- A philosophy of protection which provides a description of how this philosophy is translated into the TCB.
- A description of the interfaces between the TCB modules.
- A formal description of the security policy model enforced by the TCB which is shown to be sufficient to enforce the security policy.
- A Descriptive Top Level Specification (DTLS) which provide an accurate description of the TCB interface.
- An explanation of how the TCB implements the reference monitor concept and an explanation of why it is unbypassible and tamperproof.
- An explanation of how the TCB is structured to facilitate testing and to enforce least privilege.
- A Covert Channel analysis.

3.4.2 DRAWINGS

Drawings specifying required MLS-IAS hardware interconnections to insure secure system operation will be prepared in accordance with MIL-T-1000B.

3.4.3 TECHNICAL MANUALS

Technical manuals will be prepared in accordance with the requirements for the IAS. In addition, a Security Features User's Guide and a Trusted Facilities Manuals will be prepared in accordance with the requirements of the DoD 5200.28-STD.

3.4.4 SOFTWARE SUPPORT DOCUMENTATION

All software support documentation will be in accordance with DoD-STD-2167A, and appropriate DiDs.

3.4.5 TEST PLANS AND PROCEDURES

All test plans and procedures will be prepared in accordance with DoD-STD-2167A and applicable DIDs. Functional tests will be prepared and conducted in a manner consistent with the requirements for the IAS. In addition, testing/validation of the system security mechanisms will be conducted in accordance with the requirements of DoD 5200.28-STD. Security testing will include:

- Testing of all security mechanisms to insure they work as claimed in the system documentation
- Thorough testing by a team of knowledgeable individuals designed to uncover all design and implementation flaws
- Demonstration that the TCB is relatively resistant to penetration

These requirements may be met by a combination of vendor testing for COTS products and developer testing of the system as a whole.

3.4.6 INSTALLATION INSTRUCTIONS

Instructions for the installation of all MLS-IAS security critical software and hardware will be developed which provide detailed information on initial installation, interconnection of components, and secure operation verification. Additional instructions will be developed to inform users at each echelon of the procedures to be followed in installing non-security critical software and hardware.

3.5 LOGISTICS

3.5.1 SUPPORT CONCEPT

The support concept will be identical to that for the IAS.

3.5.2 TRANSPORTATION MODES

The MLS-IAS will be transportable in the same manner as the IAS.

3.5.3 SUPPLY SYSTEM REQUIREMENTS

The system supply concept will be identical to that for the IAS.

3.5.4 IMPACT ON EXISTING FACILITIES AND EQUIPMENT

The MLS-IAS will be designed to have minimal impact on existing facilities and equipment.

3.6 PERSONNEL AND TRAINING

3.6.1 PERSONNEL

Personnel requirements for operators and maintenance personnel will consistent for those for the existing IAS system.

3.6.2 TRAINING

Operator and maintenance training will be consistent with that for the IAS. This will be supplemented with any specialized training required to adequately inform them of specific system characteristics or restrictions which arise from the implementation of multilevel security controls.

The SysAdmin will receive a formal training course in the system security features and use of the security critical administrative tools. This will supplement training in system/database administration as provided for the IAS.

3.7 CHARACTERISTICS OF SUBORDINATE ELEMENTS

The functional and physical characteristics of the three MLS-IAS configurations were provided in sections 3.1 and 3.2.

3.8 PRECEDENCE

The order of precedence is not established.

3.9 QUALIFICATION

The MLS-IAS will meet all qualification requirements as defined for the IAS.

3.10 STANDARD SAMPLE

Not applicable.

3.11 PRE-PRODUCTION SAMPLE, PERIODIC PRODUCTION SAMPLE, PILOT, OR PILOT LOT

Not applicable.

4.0 QUALITY ASSURANCE PROVISIONS

To insure that the MLS-IAS system can be certified/accredited and maintained in a secure operating state, a Configuration Management system consistent with the requirements of DoD 5200.28-STD will be utilized during system design, development, and maintenance. In particular, the CM system will meet the following requirements:

1. During development and maintenance of the TCB, a configuration management system shall be in place.
2. The configuration management system shall maintain control of changes to the descriptive top-level specification (DTLS).
3. The configuration management system shall maintain control of changes to other design data.
4. The configuration management system shall maintain control of changes to implementation documentation.
5. The configuration management system shall maintain control of changes to the source code.
6. The configuration management system shall maintain control of changes to the running version of the object code.
7. The configuration management system shall maintain control of changes to the test fixtures.
8. The configuration management system shall maintain control of changes to test documentation.
9. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.
10. The configuration management system shall provide tools for generation of a new version of the TCB from source code.
11. The configuration management system shall provide tools for comparison of a newly generated TCB version with the previous in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

It is expected that the vendors of the COTS Trusted components will fully meet these requirements. The MLS-IAS developer must provide this capability for any developmental TCB extensions and interfacing of Trusted components in a manner not supported by the COTS vendor.

4.1 RESPONSIBILITY FOR INSPECTION

Responsibility for inspection will be consistent with that for the IAS.

4.1.1 PHILOSOPHY OF TESTING

The general philosophy of testing for the MLS-IAS will be consistent with that for the IAS. In addition, the system will fully meet all security related test requirements as specified in DoD 5200.28-STD. This requires that the system be thoroughly tested by a team of knowledgeable individuals to insure that the system security mechanisms work as claimed, that all implementation flaws be detected and corrected, and that the TCB be found relatively resistant to penetration.

It is assumed that each of the COTS Trusted components will have been independently tested and certified. MLS-IAS developmental security testing will therefore focus on testing for protection flaws introduced by the composition of the selected components or by developmental TCB extensions.

4.2 SPECIAL TESTS AND EXAMINATIONS

4.2.1 QUALIFICATION METHODS

The qualification methods will be consistent with those for the IAS and the requirements of DoD 5200.28-STD for security critical elements.

4.2.2 WAIVER OF INSPECTION

MCRDAC has the authority to waive inspection. In this case, the developer will furnish certified test data to demonstrate compliance of the system with all requirements.

4.2.3 TESTING

Testing will be conducted in accordance with the requirements for the IAS and the requirements of DoD 5200.28-STD for verification of security functionality.

4.2.4 ENVIRONMENTAL TESTING

The MLS-IAS will be subject to environmental testing consistent with that required for the IAS which is based on the general requirements of MIL-STD-810E.

4.2.5 TRANSPORTABILITY TESTING

Transportability testing will be conducted in a manner consistent with the requirements for the IAS.

4.2.6 MAINTAINABILITY VERIFICATION

Maintainability verification will be conducted in accordance with the IAS requirements.

4.2.7 INSTALLATION TESTING AND CHECKOUT

Testing of the installed system will be conducted to demonstrate that the system is operational and meets all system requirements.

4.2.8 FORMAL TEST CONSTRAINTS

The MLS-IAS will be tested using production hardware and software configured in a manner consistent with the anticipated garrison/shipboard/field deployment. All testing will be conducted using MCRDAC approved test plans and procedures and under real or approved simulations of anticipated operating conditions.

5.0 PREPARATION FOR DELIVERY

Preparation for delivery will be in accordance with the requirements for the IAS.

6.0 NOTES

6.1 ACRONYMS

ACL	Access Control List
ATACC	Advanced Tactical Air Control Central
ATARS	Advanced Tactical Aerial Reconnaissance System
ATCCS	Army Tactical Command and Control System
AVN	Aviation
C2	Command and Control
C2FAC	Command and Control Facility
C3I	Command, Control, Communications and Intelligence
C4I	Command, Control, Communications, Computers and Intelligence
CMS	Collection Management System
COC	Combat Operations Center
COMPUSEC	Computer Security
COMSEC	Communications Security
CSS	Combat Service Support
CSSE	Combat Service Support Element
DAC	Discretionary Access Control
DCT	Digital Communications Terminal
DMD	Digital Message Device
DNSIX	DODIIS Network for Security Information Exchange
DNVT	Digital Non-Secure Voice Terminal
DOD-STD	Department of Defense Standard
DODIIS	Department of Defense Intelligence Information System
DTEP	DODIIS Tactical Exploitation Program
EA	Evolutionary Acquisition
ESS	Electronic Intelligence Support System
FIREFLEX	Marine Flexible Fire Support System
FMF	Fleet Marine Force
FTP	File Transfer Protocol
GENSER	General Service
HUMINT	Human Intelligence
INFOSEC	Information Security
INT	Intelligence
IP	Internet Protocol
JSIPS	Joint Services Image Processing System
LAN	Local Area Network
MAC	Mandatory Access Control
MAFATDS	Multi-Service field Artillery Tactical Data System
MAGIS	Marine Air Ground Intelligence System
MAGTF	Marine Air Ground Task Force

MAP	Master Acquisition Plan
MCASS	MTACCS Common Applications and Support Software
MCHS	MTACCS Common Hardware Suite
MCRDAC	Marine Corps Research, Development and Acquisition Command
MCTSSA	Marine Corps Tactical System Support Activity
MDS	Meteorological Data System
MDSS	MAGTF Deployment Support System
MEB	Marine Expeditionary Brigade
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MEWSS	Mobile Electronic Warfare Support System
MIFASS	Marine Integrated Fire and Air Support System
MILOGS	Marine Integrated Logistics System
MLS	Multilevel Secure
MTACCS	Marine Tactical Command and Control System
MTS	Marine Tactical System (Message Protocols)
NDI	Non-Developmental Item
PIP	Product Improvement Program
PLI	Position Location Information
PLRS	Position Location Report System
PT-PT	Point to Point
RECON	Reconnaissance Sources
ROC	Required Operational Capability
SCI	Sensitive Compartmented Information
SCR	Single Channel Radio
SIDS	Secondary Imagery Dissemination System
SMTP	Simple Mail Transport Protocol
SSCC	Special Security Communications Center
TACC	Tactical Air Command Center
TADIL	Tactical Digital Information Link
TAOM	Tactical Air Operations Module
TCAC	Technical Control and Analysis Center
TCB	Trusted Computing Base
TCC	Tactical Communications Center
TCO	Tactical Combat Operations System
TCP	Transport Control Protocol
TERPES	Tactical Electronic Reconnaissance Processing and Evaluation System
TOPO	Topographic
TPCS	Team Portable COMINT System
TRAMPS	Tactical Reconnaissance And Message Processing System
TRE	Tactical Receive Equipment
TRSS	Tactical Remote Sensor Suite

ULCS	Unit Level Circuit Switch
ULTDS	Unit Level Tactical Data Switch
USMTF	U.S. Message Text Format
VTP	Virtual Terminal Protocol
WAN	Wide Area Network

6.2 BIBLIOGRAPHY

"Hardware/Software Architecture Recommendations for MTACCS - Draft Version 1.0," Batelle Pacific Northwest Laboratories (PNL), Richland, WA., 17 December 1990

"Information Systems Security. Products and Services Catalogue," National Security Agency, October 1990.

"Network Multi-level Security Architecture for Deployable Systems," Army Development and Employment Agency, 1 June 1988.

"Standard for Interoperable Local Area Network (LAN) Security (SILS)," For Comment Draft, IEEE 802.10 LAN Security Working Group, 25 April 1989.

Barker, "User-to-User Protection Enhances Network Security," Signal, January 1991, pp53-59.

Dillaway and Haigh, "A Practical Design for a Multi-Level Secure Database Management System," Proceedings of the Second Aerospace Computer Security Conference, June 1986.

Freeman, Neely, and Dinolt, "An Internet System Security Policy and Formal Model," Proceedings of the 11th National Computer Security Conference, October 1988.

Herbison, "Security on an Ethernet," Proceedings of the 11th National Computer Security Conference, October 1988.

Hinke, et al, "A1 Secure DBMS Design," Proceedings of the 11th National Computer Security Conference, 1988.

Karger, "Open Systems Help to Enforce Security Policies," Signal, January 1991, pp 23-26.

La Padula, et al, "DNSIX Interface Specifications, Version 2," Mitre, MTR10684, April 1990. (DIA Document No. DDS-2600-5984-90).

La Padula, et al, "DNSIX Detailed Design Specification, Version 2," Mitre, MTR10704, April 1990. (DIA Document No. DDS-2600-5985-90).

Lunt, "The SeaView Formal Top Level Specifications," SRI International, 1988.

Stoneburner and Snow, "The Boeing MLS LAN: Headed Towards an INFOSEC Security Solution," Proceedings of the 12th National Computer Security Conference, October 1989.

Wilson, "A Security Policy for an A1 DBMS (a Trusted Subject)," Proceedings of the 12th National Computer Security Conference, 1989.

6.3 GLOSSARY OF COMPUTER SECURITY TERMINOLOGY

Access - A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Approval/Accreditation - The official authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

Audit Trail - A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

Authenticate - To establish the validity of a claimed identity.

Automatic Data Processing (ADP) System - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing and retrieving data with a minimum of human intervention.

Certification - The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Channel - An information transfer path within a system. May also refer to the mechanism by which the path is effected.

Covert Channel - A communication channel that allows a process to transfer information in a manner that violates the system's security policy. See also: Covert Storage Channel, Covert Timing Channel

Covert Storage Channel - A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Cover Timing Channel - A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

Data - Information with a specific physical representation.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Descriptive Top-Level Specification (DTLS) - A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

Domain - The set of objects that a subject has the ability to access.

Dominate - Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset.

Exploitable Channel - Any channel that is useable or detectable by subjects external to the Trusted Computing Base.

Formal Security Policy Model - A mathematically precise statement of security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a

TCB, the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include state transition models, temporal logic models, denotational semantics modes, and algebraic specification models. An example is the model described by Bell and La Padula in reference [2]. See also: Bell - La Padula Model, Security Policy Model.

Least Privilege - This principle requires each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mandatory Access Control - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity.

Multilevel Device - A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

Multilevel Secure - A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are:records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

Object Reuse - The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media must contain no residual data from the previously contained object(s).

Output - Information that has been exported by a TCB.

Password - A private character string that is used to authenticate an identity.

Penetration Testing - The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users.

Process - A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.

Protection-Critical Portions of the TCB - Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects.

Reference Monitor Concept - An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Resource - Anything used or consumed while performing a function. The categories of resources are time, information, objects (information containers), or processors (the ability to use information). Specific examples are CPU time, terminal connect time, amount of directly-addressable memory, disk space, number of I/O requests per minute, etc.

Security Kernel - The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Level - The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Relevant Event - Any even that attempts to change the security state of the system, (e.g., change discretionary access controls, change the security level of the subject, change user password). Also, any event that attempts to violate the security policy of the system (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file).

Security Testing - A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also: Functional Testing, Penetration Testing, Verification.

Sensitive Information - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Sensitivity Label - A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.

Simple Security Condition - A Bell-La Padula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

Single-Level Device - A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, sensitivity labels do not have to be stored with the data being processed.

***-Property (Star Property)** - A Bell-La Padula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. Also known as the Confinement Property.

Storage Object - An object that supports both read and write accesses.

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

Subject Security Level - A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user the subject is associated with.

TEMPEST - The study and control of spurious electronic signals emitted from ADP equipment.

Trap Door - A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g., a special "random" key sequence at a terminal).

Trojan Horse - A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the Trojan Horse.

Trusted Computer System - A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Path - A mechanism by which a person at a terminal can communication directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software.

Trusted Software - The software portion of a Trusted Computing Base.

User - Any person who interacts directly with a computer system.

6.3 APPENDICES

APPENDIX A. SECURE OPERATING SYSTEM TECHNOLOGY

This appendix provides an overview of commercial Trusted operating system technology. It is not intended to be an exhaustive review, but rather to serve as an indication of emerging technology trends and available products at the time of publication of this document. Only systems which are Unix compliant, or provide at least a partially compliant interface, are included. A summary of products and known developmental efforts are shown in Table A-1. This is organized in order of the target rating for the product and no relative measures between the products are implied.

Table A-1. Overview of UNIX/POSIX Trusted Operating Systems

VENDOR	PRODUCT	API	TARGET RATING	STATUS	PLATFORMS
AT&T	SYS V R3.2/ES	SVID R3.2/POSIX	B1	CERTIFIED	3Bx,386WGS, 16 Other vendors have licensed
ADDAMAX	B1ST	SVID OR BSD	B1	AVAILABLE; ACMW IN EVALUATION	80386/486
SecureWare	SMP+	SVID/POSIX	B1	CMW+ (based on Apple AU/X) *CERTIFIED*	MAC II
SCO	SECURE UNIX	SVID/POSIX	B1	SMP+ PORT TO SYS V FY91	80386/486
OSF	OSF/1	POSIX	B1	DEV. (MACH & SMP+ BASED)	HP, DEC, ... WILL USE
SUN	SunOS MLS	BSD/SVID/POSIX	B1	AVAILABLE; EVALUATION	SUN-3 (68030) SPARC IN BETA 1Q91
TIS	TRUSTED XENIX	XENIX 2.0	B2	IN FORMAL EVALUATION	IBM PC-AT & PS/2
AT&T	SYS V/MLS	SVID R4/POSIX	B2	EVALUATION; BETA VER. AVAILABLE	3B500/600 386, SPARC IN PROGRESS
OSF/TIS/CMU	T-MACH	POSIX	B3	R&D FOR DARPA	?
HFSI	SCOMP	PARTIAL SVID	A1	CERTIFIED	DSP 6
HFSI	X/STOP	PARTIAL SVID	B3	AVAILABLE; EVALUATION	DSP 6+
SCTC	LOCK	SVID R2	A1	R&D PROTO FOR NCSC	68030

A.1 B1 SYSTEMS

In the B1 arena, AT&T Unix System V Release 3.2/ES has been the dominant product. This is a complete implementation of the SVID (System V Interface Definition standard) which meets all B1 requirements, and a number of B2 requirements. Notable features include support for a multilevel windowed user interfaces using AT&T 630MTG intelligent graphics terminals, a multilevel file

system, and a multilevel mail facility. This product was formally certified by the NCSC in 1989 and has been ported to a number of platforms including AT&T's 3B series and 386WGS workstation. Sixteen additional hardware vendors have licensed the product. This product will be superseded by AT&Ts B2 System V Release 4 expected to be available in 1991.

A major recent trend in B1 class systems has been the development of a number of B1 Unix systems designed to meet the requirements of DIA's Compartmented Mode Workstation (CMW) program. These systems all meet minimal B1 class requirements and support a number of B2 mechanisms. All of these systems provide support for multilevel file systems, single and multilevel devices, security administration, and auditing. It is also a requirement of the CMW program that these systems support a multilevel windowed user interface. In the longer term, they will be required to support multilevel data communications based on the DNSIX protocol standard (see Appendix C). Among the vendors who are active in this program are SecureWare, Addamax, and Sun. A brief synopsis of their systems follows:

SecureWare. SecureWare is a small company headquartered in Atlanta, GA. They have developed a kit to allow conversion of standard Unix systems into a B1 rated Trusted system. This kit, referred to as SMP+, meets all the requirements for a B2 system, but such a rating would require that the base OS meet the B2 architectural requirements (not true of most existing Unix releases). The SMP+ technology has been licensed by Apple, Bull, Convex, Data General, DEC, HP, SCO, and others. The SMP+ technology is used as the basis for the Apple MacIntosh II base CMW product developed jointly by Apple and SecureWare. This product, referred to as the CMW+, has recently been certified as a B1 product by the NCSC. It supports a Trusted X Window/MOTIF user interface.

Addamax. Addamax is a small company headquartered in Illinois. Like SecureWare, they have developed a kit-based approach to securing standard Unix systems. Their products, referred to under the name B1st, are available for both AT&T System V (through Release 4) and for Berkeley's BSD 4.2/4.3 Unix. Addamax and Harris jointly developed a CMW product referred to as the ACMW. Harris has since ceased participation in the program. The ACMW is presently in evaluation. It is based on a Intel 80386 based workstation (PC-AT type). As with the CMW+ product, the ACMW supports a Trusted X Window/MOTIF based user interface.

Sun Microsystems. Sun has also been developing a class B1 Trusted Unix OS as part of CMW product development effort. This is referred to as SunOS MLS and is compatible with standard SunOS (both Unix System V and BSD 4.2 interfaces). They have developed a proprietary multilevel windowing system based on SunView. At the present time, this system is only available on the Sun-3 (68030) based hardware, though it should be available on SPARC platforms in early 91. It is the Sun-3 version of the system which is undergoing evaluation at the present time. It

should be noted that Sun is committed to supporting System V Release 4 as its future OS. As such, it can be expected that Sun will utilize the B2 version of this operating system in the future.

There are two recent entries into the B1 class Unix operating system arena. First, the Santa Cruz Operation (SCO) has licensed SecureWare's SMP+ B1 technology. They are presently porting that technology to AT&T's System V Release 4 product and integrating their "Open Desktop" system. This includes X Window/MOTIF based windowing and a number of popular applications. This system should provide similar capabilities to Intel processor (80386,80486) based workstations as provided by the SecureWare CMW+ product on the 68030 based MacIntosh II.

Second, the Open System Foundation has announced that its first operating system, OSF/1, will be available shortly and will meet class B1 requirements for secure operation. This is significant in that this represents the major standardization effort for Unix/POSIX compliant systems in competition with the AT&T/Sun sponsored System V Release 4 effort. The OSF/1 product is based on the MACH kernel from Carnegie Mellon University and employs the SMP+ technology from SecureWare. A number of vendors have committed to supporting this standard including DEC and HP. They have also standardized on the X Window/MOTIF user interface, though it is not known if they intend to offer a Trusted X Window kernel as a part of the standard product.

A.2 B2 SYSTEMS

In comparison with the B1 class systems, there are limited options available in the B2 class. The first Unix-like product developed for use at B2 was Trusted Xenix. This was originally developed by IBM, however, they sold the rights to the product to Trusted Information Systems (TIS) who has continued the formal certification process with the NCSC. TIS is a small business specializing in providing expert consulting and development services for Trusted systems. The primary drawback of this product relative to the others discussed is its Xenix basis. Xenix is a Unix subset designed to run on small personnel workstations. It is limited in capabilities relative to both System V and BSD Unix and is not POSIX compliant. A multilevel Trusted user interface is not available.

The AT&T System V Release 4/MLS product is likely to become the dominant Unix product at the B2 level. This system is fully compliant with the SVID Release 4 (which includes POSIX) and a number of major vendors have committed to supporting this standard. The system is in developmental evaluation and is available to developers. AT&T is committed to porting the system to its 3B line of computers and will certify these implementations at the B2 level. As with their B1 product, multilevel windowing support will be provided using the 630MTG graphics terminal. Other vendors are committed to porting the system to SPARC based workstations,

Intel based workstations, etc. These products have not been formally announced, though it is expected they will be available in the next year.

A.3 B3 AND BEYOND

At the B3 and higher assurance levels there are limited OS products available and in development. We include them here for completeness. The Honeywell (now HFSI) SCOMP system is the only OS to have received the A1 rating from NCSC. It runs on proprietary hardware, a modified version of the Honeywell DSP 6 mini-computer. It has not been widely used due to reliability and performance problems. It does, however, provide a limited Unix interface subset. The HFSI X/STOP system is the successor to the SCOMP. It provides a similar programming interface and runs on a standard BULL DSP 6+ mini-computer. It is presently in evaluation at the B3 level.

There are also two significant government sponsored R&D efforts underway. First is the DARPA sponsored B3 Trusted MACH (TMACH) system. This is being developed by a team comprised of OSF,CMU, and TIS scientists. The goal is to provide a Unix compatible distributed computing environment which meets B3 security requirements. A B3 compliant X Window user interface is being developed as part of that program. The second is the NCSC sponsored LOCK program. This is aimed at developing a system which exceeds the A1 requirements for assurance. It is based on a commodity 68030-based computer and the LOCK/OS which provides a SVID Release 2 programming interface. A major feature of this system is the use of embedded cryptography to support on-line encryption of magnetic media and communications links. These programs could provide significant advances in security technology for the needs of future tactical automation systems

A.4 SUMMARY

At the B1 level, the AT&T System V release 3.2/ES and the SecureWare technology, as seen in the CMW+ program, OSF/1, and SCO Unix products, represent the dominant systems. However, we note that all of the B1 products discussed would be adequate to support the development of a prototype B1 class MLS-IAS. The principle differences in these products are found in the details of their Trusted Applications Interface, as no standards for this interface yet exist. This means that Trusted applications developed to work with one OS may not be easily portable into another environment. These systems also vary in terms of their file system semantics, administrative interface, audit formats, etc. These become significant if one is attempting to utilize products from different vendors within a single system, principally in terms of training and administrative workload.

At the B2 level, the new AT&T System V/MLS product clearly represents the product of choice. With the backing of major system vendors such as AT&T and Sun, its continued development and enhancement is assured. It also represents the only system likely to be available in the near term which meets POSIX interface

standards. A present weakness is the lack of Trusted X Window implementation and the limited number of platforms to which it has been ported. This situation can be expected to change fairly rapidly.

APPENDIX B. SECURE DATABASE MANAGEMENT SYSTEM TECHNOLOGY

This appendix provides an overview of secure database management system technology. It is not intended to be an exhaustive review, but rather to serve as an indication of emerging technology trends and available products at the time of publication of this document. Only Trusted relational database management systems (RDBMS) designed to meet the B1 or higher assurance class have been considered.

We note that there are no evaluated RDBMS products available at the present time, though a large number are in development or awaiting evaluation. It is expected that a number of C2 and B1 RDBMS products will enter formal evaluation during 1991. This is dependent upon the NCSC approving the draft Trusted Database Management System Interpretation (TDI). Once this criteria interpretation is approved, the evaluation process can commence. It is anticipated that the approved TDI will be consistent with the draft version presently available for comments.

There are only four announced products targeted at the B1/B2 level. These are summarized in Table B-1. As noted, Oracle is known to be conducting R&D related to products at these levels. However, they have made no product announcements. There are also several efforts underway which are working on systems at the A1 level. TRW has an internal R&D efforts working on an A1 RDBMS. From published information, it does not appear likely that this will lead to a product in the near term. One of the most advance A1 efforts is the SeaView program sponsored by the USAF/Rome Labs. A team consisting of SRI, Gemini, and Oracle is building a prototype which should be available in FY92. This system will run on the proprietary GEMSOS OS. A similar effort, also under USAF sponsorship is LOCK Data Views (LDV). This was started as a parallel effort with SeaViews and is designed to run on the NCSC sponsored LOCK system. The LOCK prototypes have been completed and an LDV prototype development effort is expected to start in FY92. The principle value of these system will be in extending the technology base which will allow the development of commercially viable RDBMSs at the higher assurance levels.

Of the four systems identified in Table B-1, three distinct architectural approaches are evident. These include a dedicated server architecture exemplified by Sybase, a Trusted front end approach used by TRUDATA, and a layered DBMS application approach used by both ITI and Informix. Based on an initial review, it appears that each of these products would provide adequate support to allow development of an initial MLS-IAS capability. However, there are significant differences in the support provided by each system, their potential performance, and design implications for other system elements. The subsequent material provides a brief summary of the significant features of each of these systems.

Table B-1. Overview of Trusted Relational Database Management Systems

VENDOR	SYBASE	ARC	ITI	INFORMIX
PRODUCT	Secure SQL Server	TRUDATA	TRUSTED RUBIX	OnLine/ SECURE
ARCHITECT.	DB Server; Dedicated HW	DB Front End	RDBMS APP	RDBMS APP
TGT RATING	B1 & B2	B1	B2 & B1 Distributed Version	B1 (B2 IN DEV.)
REQ. SUPT.	DEC VAX HW (Portable to other platforms)	SYS V/MLS SunOS/MLS + COMPAT. RDBMS	SYS V R4/ES	B1 UNIX
INTERFACE	SQL + EXT.	SQL + EXT. C-LANG.	SQL + EXT. C-LANG.	SQL + EXT. C-ISAM
MAC	Rows	Views	Rows	Rows
DAC	DB, Table	DB, Table, Views	DB, Tables	Tables, Columns
DATA TYPES	NUM, TXT, BINARY, BOOL, $, DATE, TIME, BLOB	DEPENDENT ON RDBMS	NUM, TXT, TIME, $, BOOL, NULL	NUM, TXT, DATE, $, BLOB
COMMENTS	High performance centralized DB on network. Dedicated HW and lack of local DB supt. a drawback.	Allows use of existing RDBMS. Processing overhead, limits on stored procs and triggers a drawback.	Supports historical queries. Product maturity and performance unknown.	Can serve as high performance server and local DB.
STATUS	Available	Available	Proto. Avail (3B600)	Available 2Q91

Notes:
1) No DBMS products have yet been evaluated by NCSC. They are scheduled to finalize the TDI and begin evaluations in April 91.
2) Oracle is known to be working on a number of secure RDBMS design efforts. They have not, however, announced any specific product plans.
3) SRI/ORACLE/GEMINI, SCTC, and TRW are all working on A1 RDBMS systems. The SRI SeaViews prototype should be available in FY92, the SCTC LDV design will be prototyped under USAF sponsorship starting in FY92.

B.1 SYBASE SECURE SQL SERVER

The Sybase Secure SQL Server represents a secure version of their standard SQL server product. It is fully compatible with the standard product in terms of the programming interface. Versions meeting both the B1 and B2 class requirements are being developed and they will provide an identical external interface. The existing prototype, which will presumably be the first product they will attempt to certify, is a B1 class system running on DEC MicroVax hardware. The SQL server runs on top of a B1 class OS modified by Sybase to support the server. Note that this provides a custom environment which will support no additional applications. The advantage of this architecture is that it can potentially provide higher performance and Sybase does not need to support multiple Trusted APIs.

The SQL server maintains its own unique security databases, and provides a unique administrative interface. It performs its own user identification and authentication services and enforces MAC and DAC. MAC is enforced at the row level and DAC at the database and table level. The primary interface is via ANSI standard SQL requests. SQL extensions are provided for security relevant functions. It should be

noted that the SQL server enforces DAC based on its internal security databases, and the SQL "Grant" and "Revoke" semantics are ignored.

The secure SQL server supports the following functionality:

- Support for multiple simultaneous transactions
- User defined forms and reports
- Pre-compiled procedures and triggers
- Input rules for validation and default values
- Support for BLOBs (Bit-Level Objects) up to 2 GB in size
- Auditing of security events
- Downgrading controlled by the System Administrator
- On-line maintenance and recovery

B.2 ATLANTIC RESEARCH TRUDATA

TRUDATA represents a B1 class Trusted database front end. The origin of such systems goes back to the Integrity Lock concept developed under Air Force sponsorship in the early 1980s. The basic concept employs a standard commercial RDBMS which is run as a protected subsystem. This requires that a Trusted OS be employed which will allow the RDBMS and all of its data structures and databases to be isolated and protected from direct access except via the Trusted front end. The front end, accepts user requests and translates them for the supporting RDBMS. On writes, a sensitivity label is appended to the data record, and "sealed" using a highly reliable and unspoofable method (such as encrypted checksums). On reads, the data and its sensitivity label are read, and the authenticity seal checked to insure that the data has not been modified.

The main advantage of this approach is that one can use standard commercial RDBMS technology. Hence, one can preserve the investment in existing databases, with some limitations. The primary disadvantages of this approach is in performance. Both the Trusted front end and the RDBMS must be running and all database requests must be "translated" by the front end in addition to the normal processing by the RDBMS. This "translation" would include mapping from SQL semantics supported by TRUDATA to a "Trusted" SQL request which can be passed to the native SQL RDBMS with computation of authenticity seals for each record handled as a minimum. Note also that TRUDATA MAC enforcement requires that the RDBMS and TRUDATA always exchange complete data records, else the sensitivity labels can not be authenticated. This implies that certain relational operations (e.g., projections) may require TRUDATA intervention. This design also means that stored database procedures and triggers are not generally supportable since these could alter database data but would be unable to update the authenticity seals.

TRUDATA represents a fairly sophisticated implementation of the basic concept defined above. It utilizes the security databases of the supporting Trusted OS as the basis for enforcing MAC and DAC. These are mapped onto primary views into the database tables. A primary view is a logical subset of the data which has a one-to-one mapping to the database tables. These primary views define the database record structure as perceived by the user. Only primary views of the database can be updated. TRUDATA also supports read-only derived views, which represent logical views of the data which can be formed through manipulation of the primary views. To address certain types of covert channels which exist in systems of this type, TRUDATA supports commutative filtering techniques. This can affect performance, but is largely transparent to the end user.

TRUDATA supports a number of B1 Trusted OS and commercial RDBMS products at the present time. This includes the AT&T System V/MLS and SunOS/MLS operating systems and the ShareBase and Sybase SQL servers. They are also working on interfaces to the INGRES, ACCELL/SQL, and ORACLE RDBMS products. The database features supported by TRUDATA are generally those supported by the RDBMS.

B.3 ITI TRUSTED RUBIX

The Trusted RUBIX development effort is a joint program by ITI and AT&T being supported under an Air Force R&D program. The effort is developing a Trusted version of the exiting RUBIX RDBMS which will run as a standard application on AT&T's System V Release 4/MLS B2 operating system. A standalone version of the product is targeted to run at the B2 level. A distributed database version is also being developed which will run at the B1 level.

The advantage of the Trusted application architecture is that the RDBMS can be integrated into hosts supporting a range of user applications. This avoids the need for dedicated hardware. It also has the potential to provide higher performance than the Trusted front end approach, though is unlikely to provide the performance achievable by a dedicated system such as the Sybase Secure Server. Like TRUDATA, RUBIX utilizes the security databases maintained by the OS as its basis for security enforcement. This includes the sensitivity level definition, user identification information, etc. Trusted RUBIX provide DAC enforcement at the Database and Table level and MAC at the Row level.

The interface to Trusted RUBIX is via extended SQL semantics. A C-language interface library is also provided. The system supports most commonly used data field types. It is notable that it does not support variable length text and BLOBS. Unusual features include fully integrated on-line transaction logging and recovery facilities and support for queries on historical data. It also supports view mechanisms, similar to those for TRUDATA, but employs intelligent update

processing to allow update to a large class of derived views while ensuring database consistency and integrity. Other features include:

- Support for multiple simultaneous transactions
- User defined forms and reports
- Pre-compiled procedures and triggers
- Input rules for validation and default values
- Auditing of security events
- Downgrading controlled by the System Administrator

B.4 INFORMIX ON-LINE/SECURE

Informix is presently developing a B1 and B2 class version of their On-Line RDBMS product. The B1 version will be available in the second quarter of 1991 and will presumably be submitted to NCSC for evaluation when the TDI is finalized. These products will be fully compatible with the user interface and tools available for the standard product. Architecturally, the Informix approach is similar to Trusted RUBIX. On-Line/SECURE is being designed to run as a Trusted application on top of a Unix compliant B1 or B2 operating system. It is expected that it will support at least the AT&T and OSF/1 operating systems.

Security enforcement is similar to that described above for RUBIX. The RDBMS will utilize the security databases maintained by the OS. A somewhat more fine-grained DAC mechanism is provided which will allow access restrictions to be enforced at the Table and Column level. MAC is enforced at the Row level.

The system supports an extended SQL interface and provides a C-ISAM library for direct interface to the databases from applications code. Typical data field types are supported as well as variably sized BLOBs. The size of the supported databases is principally limited by available disk space. Other features include:

- Support for multiple simultaneous transactions
- User defined forms and reports
- Pre-compiled procedures and triggers
- Input rules for validation and default values
- Auditing of security events
- Downgrading controlled by the System Administrator
- On-line maintenance and recovery
- Disk mirroring

APPENDIX C. SECURE NETWORKING TECHNOLOGY

This appendix provides an overview of secure networking technology. It is not intended to be an exhaustive review, but rather to serve as an indication of emerging technology trends and available products at the time of publication of this document. Only products designed to provide B1/B2 class network services to a network comprised of multiple heterogeneous hosts, as identified in the Trusted Network Interpretation, NCSC-TG-005, are included. We provide a brief overview of relevant products and technologies in the subsequent material.

C.1 NETWORK SECURITY DEVICES

C.1.1 Verdix Corporation VSLAN 5.0

The VSLAN is the only commercially available Trusted networking component evaluated at the present time. It has been certified as a B2 MDIA component (August 1990). The VSLAN provides:

- Secure datagram services
- MAC enforcement (16 levels and 64 categories)
- DAC (based on host identification)
- Auditing
- DES encryption for datagram integrity

It provides layer 1-2 services (as defined in the ISO protocol model) for IEEE 802.3 Ethernet. The host system may utilize either TCP/IP or OSI higher level protocol layers, transparent to the VSLAN. A single VSLAN will support up to 128 hosts.

There are two components required for a minimal VSLAN implementation, the Verdix Network Security Center (VNSC) plus a Verdix Network Security Device (VNSD) embedded in each host computer on the system. The VNSC is a PC-AT class workstation which handles all administrative interfaces and secure initialization of the VSLAN network. It runs a proprietary Verdix operating system and applications suite and will not support other processing functions. Other components include the Verdix Network Terminal Server (VNTS), which provides secure remote communications between hosts and serial user terminals, and the Verdix Secure Internet Protocol Router (VSIPR) which supports the inter-connection of multiple VSLANs or standard Ethernet LANs in a secure manner. A brief summary of the capabilities of each device is provided below.

VNSC:

- Authenticates, initializes and downloads security access rules to VNSDs
- Provides security administration and operator functions
- Provides centralized network audit collection and audit post processing
- Performs DES key management

- Provides a Trusted communication paths to other devices

VNSD:

- Acts as a memory device on the host computer bus
- Provides MAC/DAC enforcement
- Generates audit reports to the VNSC
- Encrypts datagrams using DES encryption
- Supports Multibus-1, PC-XT/AT, VME, NuBus and AT&T 3B2 architectures
- Supports Unix, VMS, and MS-DOS compliant operating systems

VNTS:

- Supports TCP/IP - Telnet protocols
- Allows connect of up to 8 serial devices with up to two connections per device
- Centronics printer support with output labelling

VSIPR:

- Provides secure datagram services between networks (standard Ethernet or VSLANs)
- Security interface for configuration and administration
- Supports ARP, ICMP, and RIP routing table updates

The VSLAN system would meet all of the requirements for the MLS-IAS LAN. However, the need to transport and maintain the VNSC workstation must be considered a drawback.

C.1.2 Boeing A1 MLS LAN

The Boeing A1 LAN is an R&D program developing a very high speed network to support large heterogeneous networks. It is designed to provide MDIA services at the A1 level. Unique features of this LAN include use of high speed (275MBPS) fiber optic transmission media and support for digital datagrams, switched digital data streams, and switched analog video data streams. The system supports both the IEEE 802.4 Token Bus and IEEE 802.3 Ethernet protocols and the DoD standard TCP/UDP/IP protocol family at the higher levels. Embedded CCEP (Commercial COMSEC Endorsement Program which provides NSA approved encryption for highly sensitive data) encryption is provided to support message integrity and end-to-end encryption to prevent information compromise. Many of these features would provide valuable adjuncts to the MLS-IAS LAN capabilities to allow for automated interfaces between systems as additional MTACCS elements achieve multilevel capability.

C.2 PROTOCOL BASED MECHANISMS

There has been a great deal of research in recent years directed at establishing requirements for secure protocol services. These efforts have been primarily oriented on mechanisms for embedding information sensitivity labels and in the application of encryption for data confidentiality and integrity. In general, these efforts have focused on the Layer 3-4 protocols (IP, TCP, TP-4, etc.), as defined in the ISO model, since this is level at which addressing and routing information is provided.

One of the major issues is the method of embedding security relevant labelling data within the protocol. For the DoD standard protocols, RFC 1038 defines a proposed Revised IP Security Option (RIPSO). This proposal has not been universally accepted due to certain limitations which resulted from the focus on defining options required to support the BLACKER program. It is however being used by DoD intelligence organizations. Efforts to define a more universally applicable IP security labelling standard are still underway. There is also an effort underway to define a standard for commercial users, referred to as the Commercial IP Security Option (CIPSO).

The DoDIIS Network for Security Information Exchange (DNSIX) protocols are designed around use of the RIPSO to provide flexible secure information exchange between cooperative hosts. Unlike the Verdix and Boeing LAN devices, DNSIX is designed to work with standard network devices with all security controls being enforced at the host level. DNSIX is designed to allow hosts to provide secure:

- File transfers
- Mail services
- Remote log-on,
- Remote processes invocation
- Remote printing
- Network managements services.

This services are accessible using the standard higher level DoD protocols (FTP, SMTP, Telnet, TCP, and UDP). To insure secure operation of the system, untrusted applications programs are not allowed to directly access the IP or lower protocol layers. Full specifications for the DNSIX protocols are available from MITRE and DIA (see Bibliography).

DNSIX will be required for all networked CMW systems. As such, a number of vendors are working on implementations. SecureWare has a prototype software implementation running which should be available this year. Addamax has a similar software implementation designed, but has not yet committed to implementation. CMC/Rockwell is developing an intelligent Ethernet card which will have embedded

DNSIX compatibility. This should provide significantly higher performance than software implementations.

Similar efforts to those described above are underway for the OSI protocol family. These are somewhat more comprehensive in that security issues relevant to applications layer services, such as X.400 secure mail, are being addressed in addition to the Layer 3-4 protocol issues. These standardization efforts are still in draft form.

NSA has an independent effort underway to define Layer 3-4 security services for the OSI protocol family. This is referred to as Secure Data Network System (SDNS). This efforts is defining the necessary protocol services to provide multilevel data services between hosts computers. This includes addressing the issues of cryptographic services for data confidentiality and integrity, cryptographic key management, and key distribution services. One of the key application of these protocols is in the development of network switches capable of handling end-to-end encrypted data traffic.

C.3 ENCRYPTION BASED PRODUCTS

There are a number of encryption based products which have been developed in recent years which are capable of supporting identification and authentication services, MAC, and DAC given appropriate key distribution controls. The approach to providing these services involves the provision of a network encryption device at each host within the system. These devices will only allow intelligible communications between hosts provided that identical cryptographic keys are in use. By providing a per-connection key, access can be controlled to very fine granularity. A centralized key distribution element can positively identify an entity wishing to communicate, using a private key, validate the requested connection based on MAC and DAC considerations, and issue a key to the two host devices for use during the communications session This obviously requires a system which supports a large number of key variables, provides over-the-air rekeying capability, and high speed encryption/decryption systems. The need to deploy and maintain a unique key management system appears to be a significant drawback to such systems in terms of the MLS-IAS application.

Available systems which can meet these requirements include:

BLACKER. This is an NSA sponsored program which provides automated network encryption and key management services for large heterogeneous networks It utilizes NSA approved encryption algorithms and can support highly sensitive data. It is an expensive and complex system which in inappropriate for small networks such as envisioned for the MLS-IAS.

Xerox XEU. The Xerox Encryption Unit (XEU) is designed to provide link level encryption services for IEEE 802.3 Ethernet LANs. It utilizes NSA approved

encryption algorithms which are suitable for highly sensitive data. The system can be set up with fixed keys at each unit, using manual distribution, to allow multiple logical networks on a single Ethernet cable. However, the device also supports over-the-air rekeying in accordance with the SDNS specifications and can provide per-session keys if an appropriate key management node is provided.

DEC DESNC. The DESNC is similar in concept to the XEU. However, it utilizes DES encryption and is designed to support commercial applications rather than high sensitive DoD applications. Utilizing a key distribution center, DEC has analyzed the security capabilities which could be provided. They determined that the system would support partial B1 functionality and can provide MDIA functionality with some restrictions on the types of supported host systems.